Lightweight Authentication Scheme for Wireless Body Area Sensor Networks

MS Research Thesis

By

Aslam Khan

Reg: # 555-FBAS/MSCS/F09

Supervised By

Prof Dr. Muhammad Sher

Department of Computer Science and Software Engineering

Faculty of Basic & Applied Sciences

International Islamic University Islamabad

1. Body area networks (Electronics)
2. Wireless LANs

A Dissertation submitted to the

Department of Computer Science and Software Engineering

International Islamic University Islamabad

In partial fulfillment of the requirements

For the degree of

Master of Science in Computer Science

2015

Final Approval

It is certified that we have examined the thesis titled "Lightweight Authentication scheme for Wireless Body Area Sensor Networks" submitted by Aslam Khan, Registration No. 555-FBAS/MSCS/F09, and found as per standard. In our judgment, this research project is sufficient to warrant it as acceptance by International Islamic University, Islamabad for the Award of MS Degree in Computer Science.

Committee

External Exam

Dr. Muazzam Ali Khan
Assistant Professor, ~~SEECS~~, EME
NUST Islamabad

30/6/15

Internal Examiner

Mr. Shahzad Ashraf Ch.
Lecturer, DCS & SE,
FBAS, IIU, Islamabad.

Supervisor

Prof. Dr. Muhammad Sher
Dean, FBAS, IIU, Islamabad

DECLERATION

It is hereby declared that this work, neither as a whole nor as a part, has been copied out from any source. It is further declared that I have conducted this research and have accomplished this thesis entirely on the basis of my personal efforts and under the sincere guidance of my supervisor Prof. Dr. Muhammah sher and my beloved teacher Mr. Shahzad Ashraf Ch. If any part of this project/thesis is proved to be copied out from any source or found to be reproduced from some other project, I shall stand by the consequences. No portion of the work presented in this dissertation has been submitted in support of any application for any other degree of this or any other university or institute of learning.

Aslam Khan

555-FBAS/MSCS/F09

DEDICATION

This thesis is dedicated to

My family who always support me morally and financially. It is also dedicated to all my beloved teachers specially Mr. Shahzad Ashraf ch, without his time and effort this thesis would not be possible to complete.

ACKNOWLEDGEMENTS

All praise to Almighty Allah Who has all the names, and Who needs no name the most generous, considerate, and compassionate Who has blessed mankind with this verdict to think, explore, to learn and discover the hidden secrets of this universe and helped me to broaden the veils of my thought and enabling me to get through the difficulties indulged during this project. Also admiration to our beloved **Prophet Muhammad (PBUH)** who is always a great source of inspiration of divine devotion and dedication to me.

I would cordially pay my special appreciations and whole heartedly considerations to my reverend supervisors **Prof Dr. Muhammad Sher** for his endless support, guidance and coordination while conducting this project. I owe him a great respect and honor and I am privileged to work under their supervision. It was their efforts, courage, moral support and endeavoring attitude that helped me to get through any problem or difficulty during each step of this project.

I would also like to pay my gratitude to all my respected teachers making me capable of what I am today due to their guidance and help. Thanking **Mr. Shahzad Ashraf Ch, Dr. Hasnain Naqvi, Mr. Shahzad Saddique** (BS Student) for their views which helped me in improving my research, also Mr. Bilal Shah for providing the managerial and administrative support.

Finally, my beloved parents and family, who deserve the credit more than I could ever express for always being completely supportive to me. They have been a constant source of advice, love and devotion to me. From moral to financial they have been blessing me with all the support that I needed up till now in my life.

Aslam Khan

555-FBAS/MSCS/F09

ABSTRACT

In past few years, Body Area Networks (BANs) became very popular in the area of healthcare, sports and military applications etc. As BAN utilizes wireless communication technologies for exchanging the critical information of patient therefore security and privacy of the patient can easily be compromised. In order mitigate these security and privacy issues, many authentication schemes have been proposed in the literature recently, but they are susceptible to potential security attacks such as server spoofing, password guessing, masquerade, denial of service, replay attacks and moreover failed to provide mutual authentication. Leu et al.'s proposed a dynamic ID-based remote user authentication scheme and claimed that their scheme is invincible against server spoofing, password guessing, and masquerade attacks.

This work reveals that the Leu et al.'s scheme suffers from correctness issues and also it does not provide mutual authentication. Leu et al.'s scheme is implemented in Wireless Sensor Network, but in this thesis an enhanced lightweight authentication scheme with respect to Tele-Medicine Information System (TMIS) is proposed. The proposed scheme is implemented in Wireless Body Area Sensor Networks. This scheme mitigates not only the correctness issues identified in Leu et al.'s scheme but also provide mutual authentication. Furthermore, a comprehensive performance and security comparison is performed in order to examine the efficiency of the proposed scheme against existing schemes. The performance comparison shows that the proposed scheme is lightweight to provide sufficient security against said potential attacks and maintains suitable computational and communication efficiency.

Chapter 1: Introduction

Chapter 2: Literature Review

Chapter 1

Introduction

1. Introduction

In this chapter a description of Wireless Sensor Network, Infrastructure of WSN and its applications is provided. Also a details description of Wireless Body Area Sensor Network (WBASN), its Constraints and Overall Architecture of WBASN is given.

1.1. Wireless Sensor Network (WSN)

WSN is one of the evolving technologies that helps human to perform various tasks such as traffic control, under water monitoring, environment monitoring and health control etc.

WSN is the combination of sensor nodes (SN) which communicates with each other and also communicates with Base Station through relay agent. Sensor nodes are small devices that have limited resources like memory, processing power, energy etc.

1.1.1. Types of Sensor nodes

Sensor nodes are divided into two categories:

- **Generic (Multi-purpose) Node**: Generic nodes collect data from the environment.
- **Gateway (Bridge) Node**: Gateway nodes pass the data collected by Generic nodes to the Base Station for processing.

WSN is the combination of Generic and Gateway nodes.

1.1.2. Infrastructure of WNS

Generally WSN is infrastructure less but it depends upon the application requirement. Followings are the two types of infrastructure:

- **Unstructured WSN:** In Unstructured WSN, sensor nodes are deployed in ad hoc or random manner with no preplanned setup. Connectivity and troubleshooting in unstructured infrastructure is difficult.
- **Structured WSN:** In Structure WSN all the sensor nodes are deployed in pre design manner on specific location. It provides easy maintenance and good coverage.

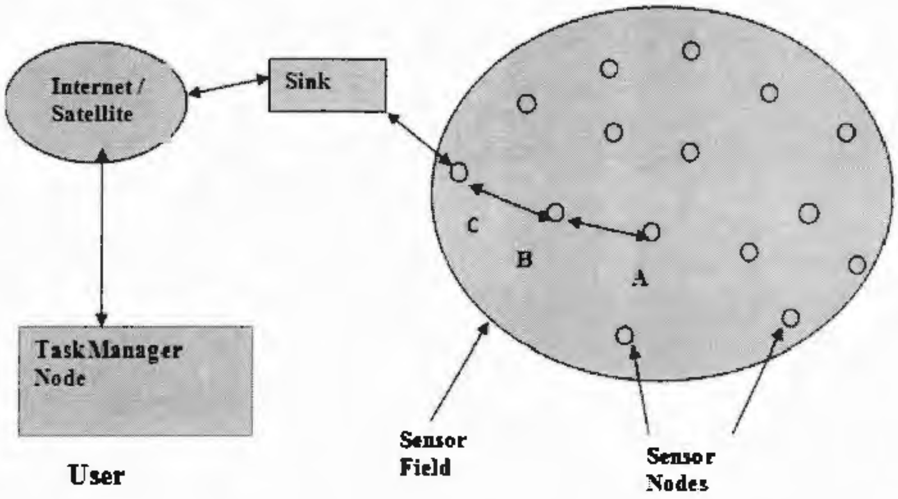


Figure 1: Infrastructure of wireless sensor networks

1.2. Wireless Body Area Sensor Network (WBASN)

Body area sensors are tiny sensors operating at radio frequency and implanted within human body to monitor human body disorders. BAS are cheap equipment but having memory, processing and power constraints, these tiny sensors are implanted in human body not to work for hours or days but for months and years, the sensors form a star topology like network in human body having many sensors and a controller (Body Central Unit) which also acts as wireless switch that receives data from all the sensors in body area and transmits the collected data to some receiver outside human body. BCU establishes an ad-hoc wireless network it provides access to all BAS, the information transmitted by in-body BCU is received by some nearby base station outside human body then the Information can be transmitted electronically to the doctor around the globe. BAS is very help full for diagnosing the irregularities in patient's body. Using the information doctor can decide medication/precaution remotely. If there is some emergency the doctor can inform patient and his/her relatives about emergency and can suggest them nearby hospital/doctor for emergency treatment.

1.2.1. Technical Constraints of WBASN

BAN is very useful but having two major drawbacks, one is its resource constraints, the second one is the security of information transmitted by Body Control Unit.

Sensor networks are having limited computations that is because of limited power. Sensors are also having low memory. In addition to these constraints physiological/biomedical sensors are restricted to size, shape and material used [4]. Even if we cope with limited power, computation and memory the sensor is useless if it cannot function properly in human body, the size and shape must be taken in mind while designing of a biomedical sensor, the material used should be biocompatible otherwise human body will start reject the sensor. All Wireless sensor networks (biomedical and otherwise) are having power restrictions[1,4], the restrictions are because of its wireless nature and its constant power ON status, as there is no wire that means no source of power is available other than some battery, which lasts for a limited time. As biomedical sensors are implanted into human body, so replacing battery means to dissect that part of the body in which the sensor was planted then change the battery of the sensor and implanted again, which is not viable.

1.2.2. Non-Technical Constraints of WBASN

There is another problem in this regard is the heat radiated from the sensor as much as power is used which can raise the temperature of the organ in one way and in the second way it will cause high blood pressure in the body and many others disorders like high metabolism of the body cells.

1.2.3. Security of WABSN

Security is one of the key factor of any system. Security is described in many ways. The Unites State DCS (Dept. of Commerce Site), describes the security as "circumstances that effect the preservation and formation of preventive operation that guarantee a state of Un-breakability from malicious operation/control".

Healthcare sensor network applications may face different security issues because the dissemination in these applications are mainly wireless in nature. Serious problems can be created for a person who are using these devices because of these attacks and threads.

As the healthcare SN application are nearly same to WSN therefor most of the security threads are also the same in both. The security issue can be categorized into two main levels, "Information security" and "System security". Threads and attacks are categorized in to "Passive attack" and "Active Attack". Passive Attack may occur during data packet sending in the system. The attacker may update the actual destination or there may be a chance of inconsistency in routing. By monitoring the Communication media the attacker can also steal the patient critical health data. In Active Attack by monitoring, the location of the user might be discover by the attacker and therefore risky circumstances can take place. Health-care system using WSN may face the following attacks.

a. Data modification

The attacker can modify part or the entire information, and transmit it to the actual receiver for some malicious purpose. Health related data are very important therefore modification to actual data can cause critical damages to patient.

b. Impersonation attack

The attacker can fraud other nodes by eavesdropping, any sensor node's identity information.

c. Eavesdropping

In Eavesdropping attack, any attacker can easily stop the radio communications between the wireless nodes. Information may be stolen for illegal act.

d. Replaying

The attacker may stole some information and after some time resend it to the receiver to accomplish dangerous purpose.

While producing Healthcare Sensor network application every security issues must be sort out. All feature of the network and its application should be covered while opposing system and information security threats.

1.2.3.1. System Security

In WBASN, from IN and OUT of the network communication, centralized controller device (CD) can be used. This CD can perform as the gateway between internal and external transmission. Firewalls, authentication and checks related to these can be taken as security measures. Security at following three levels should be applied as shown in Fig. 2.

a. Administrative Level

To manage the system, proper administrative control is important. Security measure must be taken to examine the security gaps by the people accountable for complete system operation. At this level a well-designed user hierarchy and powerful authentication mechanism may overcome the security issues. The security mechanism should be designed in such way that authorized people can only access the data. In the same way it may also be the case where data transmission should only be done to previously authorized people or place.

A star topology with all the devices associated to one centralized controller-system can reduce overhead in managing the network and it will also help in stopping DoS and Snooping attacks.

b. Physical Level Security

Measures at this level may contain access control to the data in the system and to the physical devices. In natural disaster the system may fail and may create grave situation to the overall system functionality. Therefor to make devices temper proof is important. To allow only authorized people to physical devices can be another preventive measure.

c. Technical Level Security

On hardware i.e. Server, Disks etc. checks related to technical level security are important. For safe dissemination of information server based security is required in a network in which the data is sent to central servers and at the user end client bases security is required. As health Information are very critical therefore extra steps such as data encryption and regular surveillance of the network is important.

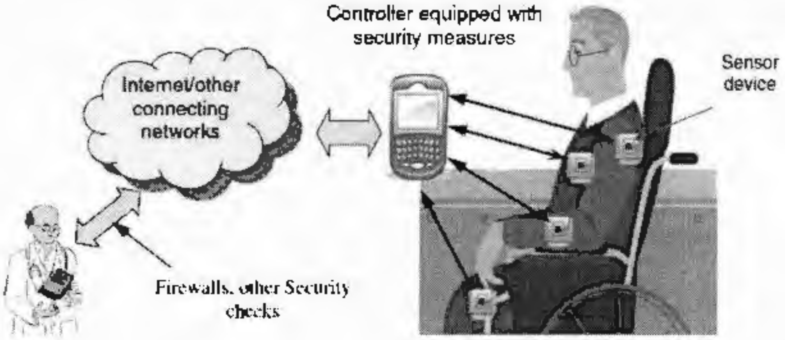

Controller equipped with security measures
Sensor device
Internet/other connecting networks
Firewalls, other Security checks

Figure 2: Gateway/Controller level Security measures in WBASN

1.2.3.2. Information Security:

Like system security information security is an important factor of WBASN, because WBASN not only contain Medical data but also patient personal data.

The responsibility of the system security mechanism is to provide the following security services to the bio-medical data.

a. Data Encryption:

To provide Confidentiality against eavesdropping attacks, data encryption is done because the data encryption stops disclosing the data while in transit.

b. Data Integrity:

Data integrity ensure the integrity of data and also data source authentication. By data integrity it can be assure that the received data in not modified. Data Source authentication is the assurance to the receiver that the data is originated by specified sender. Data integrity is an effective way against the data modification attack.

c. Authentication:

It assure association process between the nodes. Authentication is an effective way against impersonation attacks.

d. Freshness:

Freshness assure that the received data is the latest and is not the old data replaying by the attackers.

1.3. Over all Architecture of WABSN

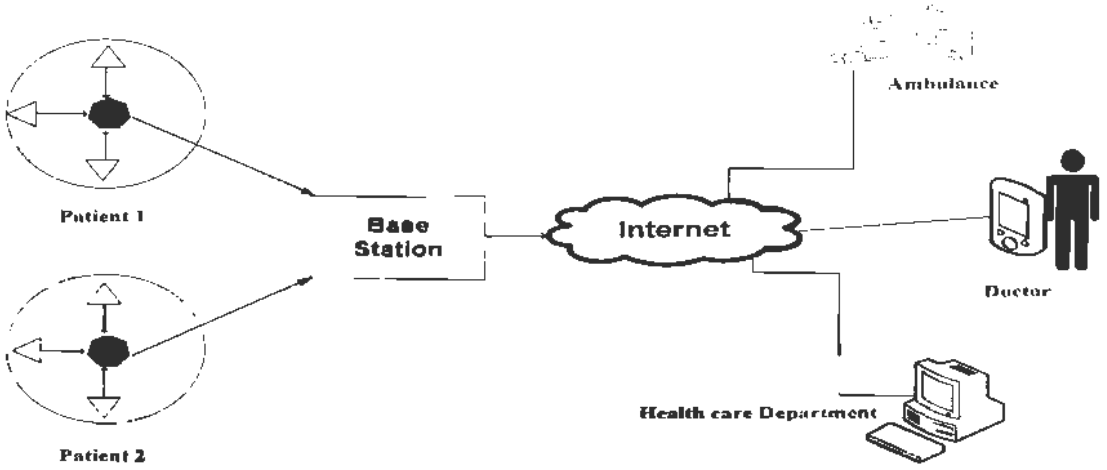


Figure 3: Over all architecture of BASN

Overall architecture of WBASN is shown in figure 3. The biosensors implanted in human body sense the patient's conditions and send the sensed information back to anchor node working as a cluster head. The anchor node is equipped with a transmitter, which transmit the aggregated data on ISM band which will be received by some base station outside the human body. The info received from the base station is connected to health care via an internet, which will further prioritize the message delivery in emergency cases to department, doctor and an ambulance service, base station will decide the destination of the message.

Upon receiving the info doctor / healthcare staff will decide what to do either to inform the patient or his relatives about the medical condition of the patient or suggesting some nearby hospital/ doctor or about precautions/ cure etc.

Chapter 2

Literature Review

2. Literature Review

Security of WBASN is important factor because patient medical data must be saved from illegal use of fraudulent act that might be dangerous for human's life. A number of security solutions have been presented for WBASN in last few years.

In 2007 Benoit Latre et al.'s in [4] a low delay protocol for multi hop WBASM, The main objective of this protocol is to route data to the destination and to provide a collision free access to medium. This goal is achieved by implementing a tree structure which ensures a collision free access to communication medium. Moreover, it is shown that CICADA is a low energy and a minimal delay protocol particularly designed for wireless. This approach focuses on energy efficiency and there is no mechanism for securing the information. In 2008 Khan et al.'s [1] proposed "Performance Evaluation of a WBASN for Remote Patient Monitoring", this scheme mainly focuses on the performance evaluation of Remote Patient Monitoring (RPM) system based on WBSN, however this scheme lacking in security of the transmission, in 2011 Mohammed Mana et al.'s [2] used physiological signals i.e. electrocardiogram (ECG) to address security issues in WBAN. They used ECG signal in WBAN for Symmetric cryptographic key generation and distribution. Their scheme has been divided into Key generation, key-setup, key authentication, and key update phases, this scheme is latter found as less energy efficient as the base station need to keep track each key pair of all the nodes. In 2009 A key distribution and management scheme has been proposed by Keoh, et al.'s [3] by using key chains to create group keys for WBASN and to adjust to membership changes, group key-update and re-keying is provided. They used one way hash functions and symmetric key encryption for the secure discovery of sensors which allows the sensor devices to interchange security information. This approach required much energy when dealing with key exchanges. In 2011 Sye Loong Keoh in [20] proposed, a novel key distribution and management scheme which is based on hash chain, one way hash function and symmetric key encryption. In this scheme, key chains are used to generate group keys for BSN and handle group re-keying and key-update to adjust to membership changes. A light weight sensor to sensor authentication scheme based of Elliptic Curve Diffie-Hellman (ECDH) is also proposed in this scheme however this scheme required high energy resources because whenever a new sensor is added to the network the controller will broadcast the existing key chains to the newly added sensor and when a sensor exit the group-key must be updated. In 2014 Zhao in [21] present an identity (ID)-based efficient anonymous authentication scheme using elliptic curve crypto-system. Zhao scheme is divided in to, Initialization, Registration and Authentication phases. They claimed that this scheme provides mutual authentication between the client and the application provider, and keeps the client anonymous as well. In 2011 Aftab Ali et al.'s in [22] proposed Keyed-Hashing MAC (HMAC-MD5) for protecting personal Info in WBAN, in which communication between nodes is secure by using EKG (Electrocardiography), for securing the process HMAC-MD5 is applied on Electrocardiography. Key agreement is done by computing HMAC-MD5 of feature block and Data encryption is done by using the generated key. Authentication is done by applying MAC on each data message whereas Freshness is achieved by applying Electrocardiography values in key agreement. In 2014 Daojing He et al.'s in [23] identified security risks in the Data disclosure and Spreading of data in WBANs and proposed a lightweight and confidential data discovery and dissemination protocol. According to the author low complexity symmetric cryptography techniques are used for maintaining the privacy and in addition the authenticity of the broadcasted data items are ensured by changing the encryption key on per packet basis to stop the intermediate nodes from extracting the key. In 2011 Lee et al.'s in [25], present a scheme to solve the security issues in Hsiang et al.'s scheme. In 2014 Jenq-Shiou Leu, et al.'s in [26] pointed out that Lee et al.'s scheme is susceptible to Masquerade, server spoofing and offline password Guessing attacks, however through detail analysis we find that Jenq-Shiou Leu, scheme's having serious problems with Registration, authentication and Password change phases.

2.1. Performance Evaluation of a WBASN for Remote Patient Monitoring [1]

This paper focuses on the performance evaluation of Remote Patient Monitoring (RPM) system based on WBSN. The main targeted metric of investigation is the delay and the research is based on the hypothesis that we can monitor a patient form a remote location with having considerable delay. The researchers have proposed two major design issues. First is that the WBAN should be kept in isolation from the hospital's network. Second, rather than using TCP, it is better to utilize a multi hop network that is composed of a hybrid topology which is a combination of wireless and fixed links to improve (as much as possible) transmission speed. The reason behind using such a topology is that small size TCP packets increases end-to-end delay. To implement a remote RPM system researcher used a star topology WBAN where all SN transmit data to the master (service) node which could combine all sensor data and send using a TCP/IP channel for reliable data transmission. All the simulation and results have been verified through OPNET simulation.

Limitations:

Authors did not consider physiological effects of in-body sensors.

There is no mechanism of securing the transmitted data.

2.2. Trusted Key Management Scheme for WBAN [2]

This paper presents an approach that uses physiological signals ((ECG (electrocardiogram) to overcome security problems in WBAN. Using ECG signals to constituent sensors in a WBAN and to protect the privacy, this approach manages the creation and distribution of symmetric cryptography keys. According to this scheme the key management has been divided into four steps; Key Generation, key setup, key authentication and key update phases. Results shows that the proposed protocol have solved the security problem and privacy problem in the WBAN. It additionally targets to securely and efficiently producing and distributing the session keys between the SN and the BS (base station) to secure end to end communication. It also allows to secure, communication channels between the nodes.

Limitations:

Authors did not consider physiological effects of in-body sensors.

Base station keeps records of each key pair of all the nodes and freshness is provided by per key message, so base station is assumed to have very large memory and high operating power.

2.3. Securing BSN: Sensor Association and Key Management [3]

A key distribution and management scheme has been proposed in this paper that uses key chains to create group keys for BSN and provide group key update and re-keying to adjust to membership changes. This approach focuses on secure discovery of sensors which allows the sensor devices to interchange security information like symmetric keys and public keys etc. it is also shown that how the sensors must be connected with the patient's devices. This scheme uses hash functions and symmetric key encryption and does not rely on asymmetric cryptography. This approach increases the efficiency with a lower computational overhead. Key update messages authentication can easily be done because of the use of hash functions. Results shows that the proposed key management scheme solves the security problem and privacy problem in the WBAN.

Limitations:

There is no mechanism of authentication of nodes message.

The protocol will require much energy when dealing with key exchanges.

2.4. A Low-delay Protocol for Multihop WBAN [4]

This paper presents a dissemination protocol for WBAN called CICADA. The core objective of this protocol is to route data to the destination and to provide a collision free access to medium. This goal is achieved by implementing a tree structure which ensures a collision free access to communication medium. Moreover, it is shown that CICADA is a low energy and a minimal delay protocol particularly designed for wireless, multi hop Body Area Network. According to this paper, CICADA sets up an autonomous tree which is then used to deliver data from the nodes to the destination or sink node. Each tree structure (cycle) is used to assign time-slots to the different nodes in a distributed way. CICADA divides such a cycle in a control sub-cycle and data sub-cycle, therefore decrease the delay and introduce mobility robustness. CICADA has been analyzed using NS-2 simulation and the results show that the protocol offers low delay. The energy utilization is low because in a time-slot in which a node is not sending or receiving, in those time-slots a node can sleep.

Limitations:

Authentication and freshness is not provided.

2.5. Body Area Sensor Networks: Challenges and Opportunities [5]

The paper described different challenges and opportunities in wireless body area network, which are size, cost, compatibility, and perceived value, the requirements for widespread use are as follows:

Value. For Perceived value many elements can be consider, like assessment ability, but in general, the WBASN must amend user's quality of life.

Safety. Wearable and inserted sensors need to be biocompatible and almost hidden to avoid damages to the user. Critical safety related applications must have fault tolerant actions.

Security. Illegal access or handling of system function could have severe concerns. Security measures such as user authentication will avoid such concerns.

Privacy. WBASN will be trusted with possibly sensitive info about people. Both technical and non-technical solutions will be required to protect user privacy.

WBASN packaging will required to be unobtrusive/hidden to avoid attention to medical conditions. To safeguard sensitive information, encryption will be necessary.

Compatibility. WBASN nodes require to inter-operate with other WBASN nodes, existing inter-WBASN, and even with electronic-health record systems. This will need calibration of dissemination protocols and data storage formats.

Ease of use. Wearable BASN nodes should be small in size, hidden, comfortable, should easily be put on and should be small in numbers. Intelligent On-body and off-body user interface control will be required as well

Limitations:

The paper is more towards survey and case study, no security mechanism is proposed in the paper.

2.6. A Novel Biometrics Method to Secure WBASN for Telemedicine and M-Heath [6]

The growth of the WBASN is extremely important for recent telemedicine and medical-health, but security remains a difficult challenge yet to be determined. As nodes of WBASN are expected to be interconnected ON/IN the human body, the body itself can compose naturally secure communication pathway that is unavailable to all other types of WN. This article discovers the use of this pathway in the security mechanism of BASN; that is, by a bio-metrics approach that utilizes an inherent characteristic of the human body as the authentication identity or the means of safeguarding the distribution of a cipher key to secure inter WBASN communications.

Limitations:

This study instead of providing a strong security mechanism opened a few important issues for future research, containing, coding schemes, schemes for the asynchrony of diverse channels, and other appropriate bio-metric traits.

2.7. Efficient Group Key Management and Authentication for BSN [20]

This paper proposed a Novel key distribution and management scheme established on Hash chain, one way hash function and symmetric key encryption. In this scheme, key chains are used to create group-keys for BSN and handle group key-update and re-keying to adjust to membership changes. A controller (PDA/mobile) in the BSN is responsible for key management and distribution. Every time a new sensor is added to the network the controller will broadcast the existing key chain to the newly added sensor and whenever a sensor exit the group key must be updated. A light weight sensor to sensor authentication scheme based of Elliptic Curve Diffie-Hellman (ECDH) is also proposed.

Limitations:

It is assumed that patient's controller is having more power and computational capabilities. This scheme is good for a network where sensors are very rarely add or leave because when sensors are frequently leave or add to the network then Patient's controller will most of the time update and broadcast the key.

2.8. An Efficient Anonymous Authentication Scheme for WBAN using Elliptic Curve Cryptosystem [21]

Author propose an identity (ID)-based efficient anonymous authentication scheme for WBANs using elliptic curve cryptosystem (ECC). Because of the ID-based concept used, certificate is required. Moreover, the proposed scheme provides mutual authentication between the client and the application provider, and keeps the client anonymous as well. The author also claiming the improvements in the Performance analysis.

The author described 3 type of participants in the authentication scheme:

1. The WBAN client, is a Patient who uses WBAN terminals i.e. PDA or AP provided Medical devices.
2. Network Manager (NM), is responsible for PK (Private Key) generator for the client and AP.
3. Application provider (AP) is a Hospital, clinic or doctor.

The author divided the proposed solution in to three phases:

i. Initialization
ii. Registration
iii. Authentication

i. Initialization:

In Initialization phase, to generate System parameters (params) NM follows the following steps

1st NM generate two large prime number p, q, an elliptic curve $E\left(F_p\right)$over F_p and a group G with order q, then NM selects four hash functions $H1(\cdot)$, $H2(\cdot)$, $H3(\cdot)$ *and* $H4(\cdot)$and then NM selects a random No $S_{MN} \in Z^*_q$and computes $Q_{NM} = S_{NM} \bullet P$. Then, NM publishes $params = \{p, q, E(F_p), G, h(\bullet), H(\bullet)\}$ as the system parameters and keeps his secret key S_{MN} secretly.

ii. Registration:

The following steps need to executed between C and NM, For a WBAN client C, to become a legal client

1. C send message $\{ID_C, X_C^1, X_C^2, X_C^3 \cdots, X_C^n\}$ to NM where ID_C is the identity of C chosen by C. $\{X_C^1, X_C^2, X_C^3 \cdots, X_C^n\}$ is a family of random numbers from Z_q^*, generated by C. For each i, C also computes $X_C^i = X_C^i P$
2. On Receiving the message the NM validate the ID_C and reject it if it's not valid otherwise NM selects a family of un-linkable pseudo identities $PID_C = \{pid_C^1, pid_C^2, \cdots pid_C^n\}$. NM also generates a family of random numbers $\{y_C^1, y_C^2, y_C^3 \cdots, y_C^n\}$ from Z_q^* . For each i, NM computes $Y_C^i = Y_C^i P$, $Q_C^i = X_C^i + Y_C^i$, $h_C^i = H_1(pid_C^i \| Q_C^i \| right)$ and $Z_C^i = y_C^i + h_C^i \cdot s_{NM}$.

   At last, NM sends all $\{right, (pid_C^1, Z_C^1, Y_C^1), (pid_C^2, Z_C^2, Y_C^2) \cdots, (pid_C^n, Z_C^n, Y_C^n)\}$ to C through a secure channel.
3. Upon receiving $\{right, (pid_C^1, Z_C^1, Y_C^1), (pid_C^2, Z_C^2, Y_C^2) \cdots, (pid_C^n, Z_C^n, Y_C^n)\}$, C computes $Q_C^i = X_C^i + Y_C^i$, $h_C^i = H_1(pid_C^i \| Q_C^i \| right)$ and checks whether the equation $Z_C^i P = Y_C^i + h_C^i \cdot Q_{NM}$ holds for each i. If one of those equation does not hold, C rejects the response, otherwise C computes $s_C^i = X_C^i + Z_C^i$ and keeps $\{right, (pid_C^1, Z_C^1, Y_C^1), (pid_C^2, Z_C^2, Y_C^2) \cdots, (pid_C^n, Z_C^n, Y_C^n)\}$ secretly.

iii. **Authentication:**

In Authentication phase the sender (WBAN client) send message $m_1 = \{A_C^i, CT, t_C^i\}$ to Receiver AP, where

$A_C^i = a_C^i.P$ (a_C^i is a random number).

$CT = E_{K_C^i}(pid_C^i \| Q_C^i \| right \| V_C^i)$.

t_C^i is the recent time stamp.

On receiving the message from C, AP verify the Freshness, if the message is not fresh AP reject the request otherwise it validate the equation $Q_C^i + h_C^i \cdot Q_{NM} + l_C^i \cdot P = V_C^i A_C^i$, if it does not hold then the AP reject the request otherwise AP compute B_C^i, Auth and SK and then send message $m_2 = \{B_C^i, Auth\}$ to C, where

$B_C^i = b_C^i \cdot P$ (b_C^i Is a random number).

$Auth = H_4(A_C^i \| \vec{A}_C^i \| B_C^i \| t_C^i)$.

$SK = H_5(Auth \| b'_C \| A'_C)$.

On receiving the message from AP, C compare Auth and $H_4(A'_C \| \bar{A}'_C \| B'_C \| t'_C)$ if both are not equal C stops the session. Otherwise C computes session key $SK = H_5(Auth \| a'_C \| B'_C)$.

Limitations:

This scheme required heavy computational and heavy communication because of the computation and communication of complete array.

2.9. A cluster-based key agreement scheme using keyed hashing for BAN [22]

The author proposed Keyed-Hashing MAC (HMAC-MD5) for protecting personal Info in WBAN, in which communication between nodes, is secure by using EKG (Electrocardiography). for securing the process HMAC-MD5 is applied on Electrocardiography (EKG), Key agreement is done by computing HMAC-MD5 of feature block and Data encryption is achieved by using the generated key.

Authentication is done by applying MAC on each data message of L-sensor and H-sensor and Freshness is achieved by applying Electrocardiography (EKG) values in key agreement.

The author is assuming a heterogonous WSN which consists of High end sensors and Low-end-sensors. H-sensor is having high resources capability and act as CH (Cluster head). L-sensors are having limited resources and acting as cluster member. Both L-sensor and H-sensor can calculate EKG.

To secure the network Keyed hashing in applied on Electrocardiography (EKG) blocks and then feature block is extracted from the Electrocardiography (EKG) signal and then quantize into binary stream. In the key agreement phase, keyed hash of Electrocardiography (EKG) data and ID of H-sensor node is applied on L-sensor & H-sensor. The keys generated by EKG, are verified using MAC verification on H-sensor.

EKG based key generation is divided into Feature Generation phase and Key Agreement phase

In the feature generation phase, DWT is used to extract features and then for inter-sensor communication the features are quantized. In the communication process between L-sensors and H-sensor 625 Hz sample of Electrocardiography (EKG) signals are produced in the duration of 5 seconds and then those 625 samples are separated into 5 (five) parts of 125 Hz each. After filtration DWT is applied. By concatenating 64 coefficients horizontally. the 320 coefficient feature vector is created. As shown in the following figure.

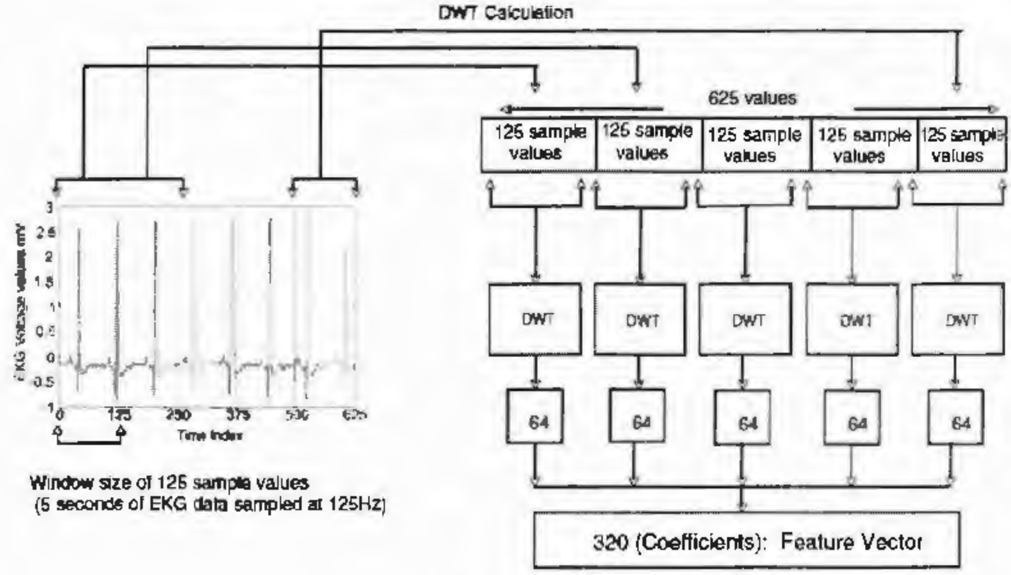


Figure 4: Feature generation.

In the Key agreement phase, after the feature file generation H-sensor releases data request message which consist ID_H, DataReq and nonce.

H → *: $ID_H, Data\,\mathrm{Re}q, nonce$

All the L-sensors compute the shared pairwise key, with H-sensor by applying one way hash function of the feature blocks, ID_H and ID_L as shown below

$K_{H,L} = HMAC((b_{11}, N)\cdots(b_{211}, N), ID_H \parallel ID_L)$.

With $K_{H,L}$, the L-sensor encrypt the data and also compute nonce from H-sensor. L-sensor then transmit its ID, encrypted data and MAC to the H-sensor.

L → H: $ID_L, E_{K_{H,L}}(ID_L, Data), MAC_{K_{H,L}}(ID_L, nonce, Data)$.

When H-sensor received the message, it calculate $K_{H,L}$ and decrypt the message with $K_{H,L}$. The message authenticity is checked by H-sensor by MAC verification with $K_{H,L}$.

After initialization and shared pairwise key generation between H-sensor and L-sensors, Cluster key is computed. To generate CK (Cluster Key) CH release a signaling message H → *: GenCK(ID_H) to L-sensor. Every L-sensor receives this message, generate CK. CK is refreshed after some fixed time, whenever the CH try to change the CK, sends message H → *: GenCK(ID_H) and L-sensor regenerates the CK upon receiving the message.

Limitations:

This scheme is less energy efficient because of the computation involved.

2.10. Lightweight Confidential Data Discovery and Dissemination for WBAN [23]

The author has identified security risks in the Data disclosure and Spreading of data in WBANs and proposed a lightweight and confidential data discovery and dissemination protocol. According to the author low complexity symmetric cryptography techniques are used for maintaining the privacy and in addition the authenticity of the broadcasted data items are ensured by changing the encryption key on per packet basis to stop the intermediate nodes from extracting the key.

The proposed protocol is divided in to 3 phases, System initialization, Packet processing and Packet verification.

i. System Initialization:

In this phase the BS (Base Station) generated more than one one-way key hash chains and loads the committed value of the hash chain on each node corresponding to the hop distance. Hash chains are based on $H(\cdot)$ function which has easy computational properly but its inverse $H^{-1}(\cdot)$ computation is very difficult. By applying $H(\cdot)$ to the starting element repeated by b time, a hash chain with b length is produced. The last value applied for b times after $H(\cdot)$ is called committed value of the hash chain. According to the hop distance from BS the nodes are divided in to N groups. Before the deployment of the nodes BS set up N hash chains by generating N different random seeds and calculate one-way hash chain with length b starting from each seed as shown in the following figure.

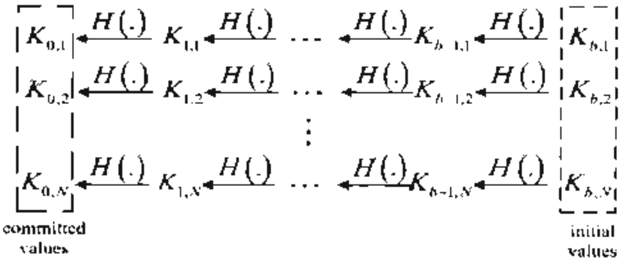

$K_{0,1}$ $H(.)$ $K_{1,1}$ $H(.)$ … $H(.)$ $K_{b-1,1}$ $H(.)$ $K_{b,1}$
$K_{0,2}$ $H(.)$ $K_{1,2}$ $H(.)$ … $H(.)$ $K_{b-1,2}$ $H(.)$ $K_{b,2}$
$K_{0,N}$ $H(.)$ $K_{1,N}$ $H(.)$ … $H(.)$ $K_{b-1,N}$ $H(.)$ $K_{b,N}$
committed values
initial values

Figure 5: Construction of multiple one-way key hash chains

Where the $(b-i)th$ output of hash function is obtained from the jth random seed number i.e. $K_{b,i}$ is represented by $K_{i,j}$. The length of b of each chain can be random but not less than the number of data items BS want to communicate in the lifetime of the network.

The committed value of the *jth* key chain $K_{0,j}$, corresponding to the hop distance j, is pre-distributed to the node in the *jth* hop group before the deployment.

Four tuple (order, Key, version, data) is used to represent the data, where 'order' is the order of data communication, (the higher order number represent latest data), the concerned variable is uniquely identified by 'key', 'version' specified whether the data item is new and the data indicates the disseminated value for the concerned variable.

ii. **Packet Preprocessing Phase:**

When the BS want to spread the data item d = {order, key, version, data}, it generates a packet through concatenating the data item d and successor key and encrypt the data with symmetric encryption technique. The packet pro-processing result P_i for the *ith* data item $(d_i = \{order_i, key_i, version_i, data_i\})$ spread to N hops is $P_i = E(\{d_i, K_{i,1}\}, K_{i-1,1}) \| \cdots \| E(\{d_i, K_{i,N}\}, K_{i-1,N})$, where $1 \leq i \leq b$ and $order_i = 1$.

iii. **Packet verification:**

On receiving a packet P_i each sensor nodes i.e. S_k recovers the correct group information from P_i i. e the node parses the right field $E(\{d_i, K_{i,1}\}, K_{i-1,1})$ and then uses the key $K_{i-1,1}$ to perform $D(E(\{d_i, K_{i,1}\}, K_{i-1,1}\}, K_{i-1,1}) = \{d_i, K_{i,1}\}$ to decrypt the cipher text and then node S_k perform the following information:

- **a.** If the received data item i.e the $order_i$ in the packet is newer than that of its stored $order_{i-1}, K_{i-1,1}$ then the S_k check whether the received key $K_{i,1}$ to the stored $K_{i-1,1}$ the authenticity and integrity of the packet is assured if the result is positive and the packet is accepted.
- **b.** If S_k has received the same data packet which is already ready received, it increase the broadcast interval of the received packet through the trickle algo.
- **c.** If an older packet (which was stored previously) is received then node S_k broadcast its stored data packet.

Limitations:

They claim it to be a lightweight but still it required high resources because of the heavy computation involved.

2.11. A secure dynamic ID based remote user authentication scheme for multi-server environment using smart cards [25]

In Lee et al.'s proposed solution, there are three core participants: U_i (user) S_j(Server) and RC. The RC is supposed to be a trusted party. The RC selects the master key x and secret number y to calculate $h(x\|y)$ and $h(y)$. Then, through secure channel the RC (Registration Center) shares $h(x\|y)$and $h(y)$ with ServerS_j. The author proposed solution is divided into Registration, Log in, Verification and Password change phases.

i. Registration Phase:

In registration phase userU_i first selects hisID_i, a random number b and PW_i and then compute $h(b\oplus PW_i)$ and then send $(ID_i, PW_i, h(b\oplus PW_i))$ to RC, on receiving $(ID_i, PW_i, h(b\oplus PW_i))$ the RC calculates:

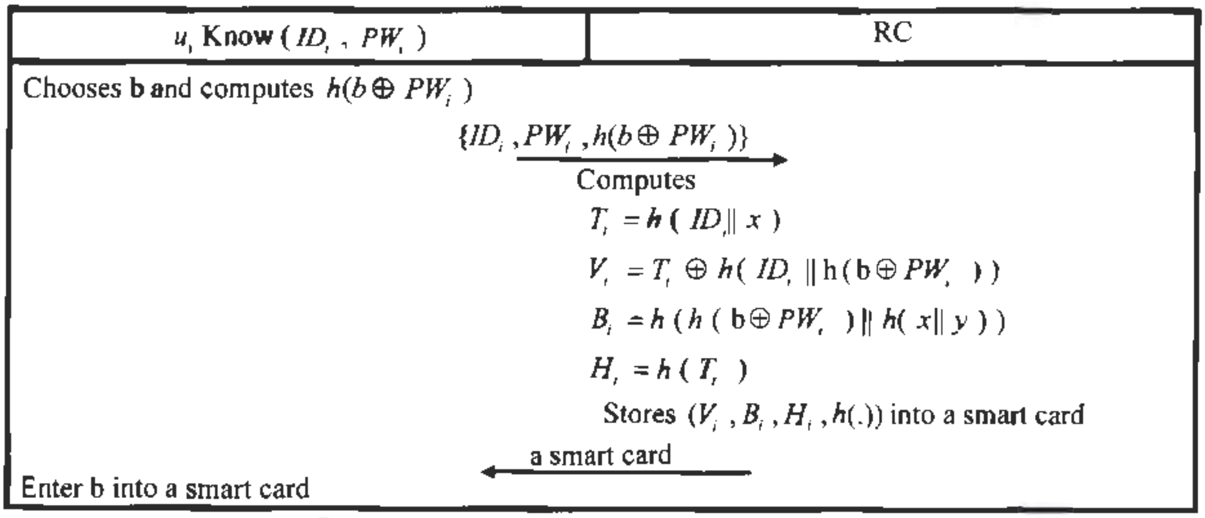
$T_i = h(ID_i \| x)$

$V_i = T_i \oplus h(ID_i \| h(b\oplus PW_i))$

$B_i = h(h(b\oplus PW_i) \| h(x\|y))$

$H_i = h(T_i)$

and store $(V_i, B_i, H_i, h(.), h(y))$ into a SmartCard and then send the SmartCard to User, the user on receiving SmartCard store b into the SmartCard.



u_i Know (ID_i, PW_i)

RC

Chooses b and computes $h(b\oplus PW_i)$

$\{ID_i, PW_i, h(b\oplus PW_i)\}$ →

Computes

$T_i = h(ID_i \| x)$

$V_i = T_i \oplus h(ID_i \| h(b\oplus PW_i))$

$B_i = h(h(b\oplus PW_i) \| h(x\|y))$

$H_i = h(T_i)$

Stores $(V_i, B_i, H_i, h(.))$ into a smart card

← a smart card

Enter b into a smart card

Figure 6: Lee et al.'s scheme's Registration phase

ii. **Log In phase:**

In this phase When User (U_i)want to login the user enter his smartcard and then insert ID_i, PW_i, the SmartCard then computes:

$$T_i = V_i \oplus h(ID_i \| \mathrm{h}(\mathrm{b} \oplus PW_i))$$
$$H_i' = h(T_i)$$

And then check $H_i' \overset{?}{=} H_i$, if equal then U_i is a legal user. The SmartCard then generate a Random number N_i .

$$A_i = h(T_i \| h(y) \| N_i)$$
$$CID_i = h(b \oplus PW_i) \oplus h(T_i \| A_i \| N_i)$$
$$P_{ij} = T_i \oplus h(h(y) \| N_i \| SID_j)$$
$$Q_i = h(B_i \| A_i \| N_i)$$

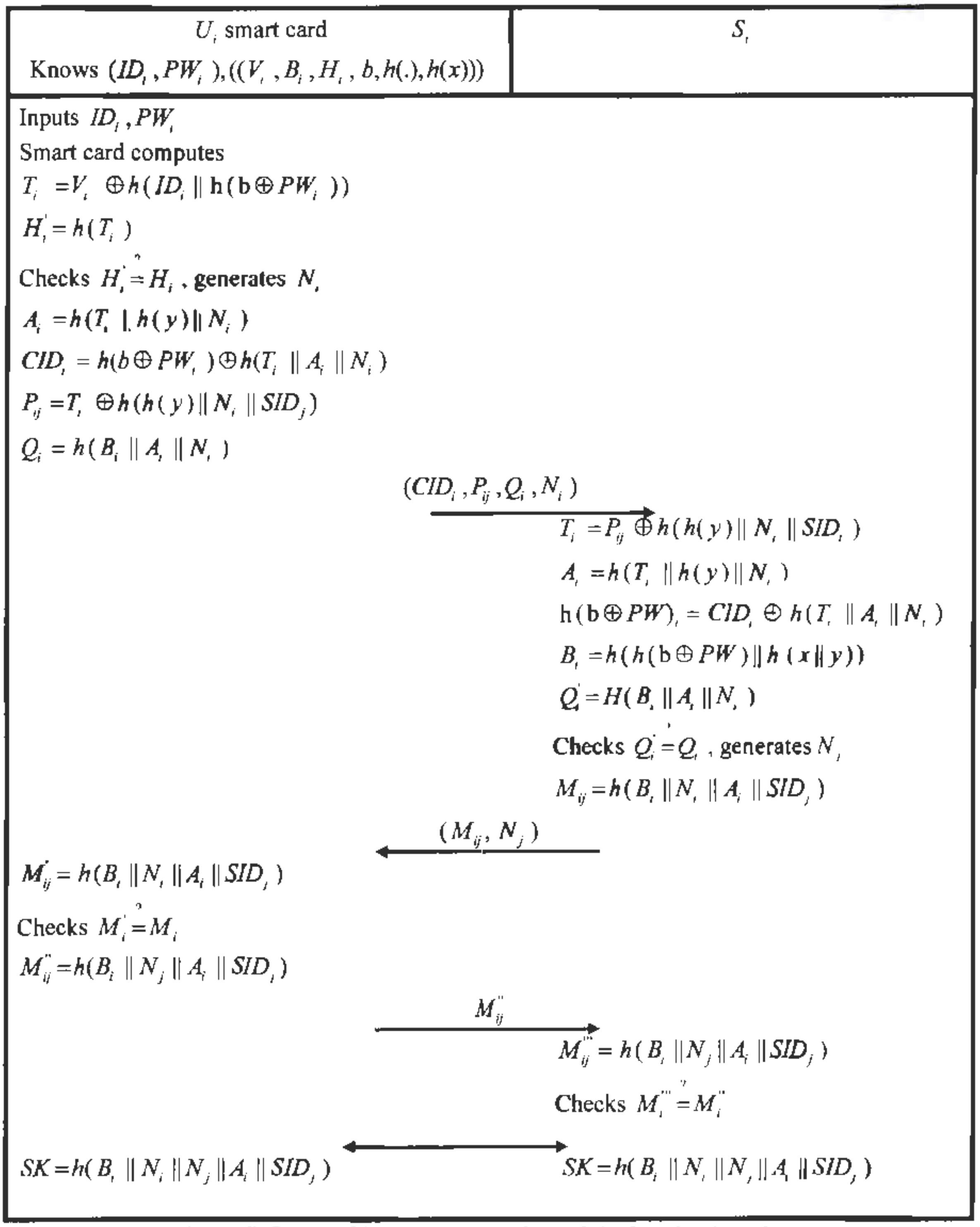
And then send $(CID_i, P_{ij}, Q_i, N_i)$ to the server.

iii. **Verification Phase:**

The server on receiving(CID_i , P_{ij} . Q_i , N_i), computes:

$$T_i = P_{ij} \oplus h(h(y) \| N_i \| SID_i)$$
$$A_i - h(T_i \| h(y) \| N_i)$$
$$\mathrm{h}(\mathrm{b} \oplus PW)_i = CID_i \oplus h(T_i \| A_i \| N_i)$$
$$B_i = h(h(\mathrm{b} \oplus PW') \| h(x \| y))$$
$$Q_i' = H(B_i \| A_i \| N_i)$$

And check $Q_i' \overset{?}{=} Q_i$, if both are not equal the server drop the login request otherwise the request is accepted and the server generate random number N_j to compute $M_{ij} = h(B_i \| N_i \| A_i \| SID_j)$ and send (M_{ij}, N_j) to the user. The user on receiving (M_{ij}, N_i) compute $M_{ij}' = h(B_i \| N_i \| A_i \| SID_j)$ and then compare $M_i' \overset{?}{=} M_i$ if both are equal the user compute $M_{ij}'' = h(B_i \| N_j \| A_i \| SID_j)$ and send M_{ij}'' to the server otherwise drop the response. The Server on receiving M_{ij}'' compute $M_{ij}''' = h(B_i \| N_j \| A_i \| SID_j)$ and then compare $M_i''' \overset{?}{=} M_i''$ if both are equal both User and Server share session key $SK = h(B_i \| N_i \| N_j \| A_i \| SID_j)$ for secure communication.



U_i smart card

Knows $(ID_i, PW_i), ((V_i, B_i, H_i, b, h(.), h(x)))$

S_j

Inputs ID_i, PW_i

Smart card computes

$T_i = V_i \oplus h(ID_i \| \text{h}(\text{b} \oplus PW_i))$

$H_i^{'} = h(T_i)$

Checks $H_i^{'} \overset{?}{=} H_i$, generates N_i

$A_i = h(T_i \,|.\, h(y) \| N_i)$

$CID_i = h(b \oplus PW_i) \oplus h(T_i \| A_i \| N_i)$

$P_{ij} = T_i \oplus h(h(y) \| N_i \| SID_j)$

$Q_i = h(B_i \| A_i \| N_i)$

$\xrightarrow{(CID_i, P_{ij}, Q_i, N_i)}$

$T_i = P_{ij} \oplus h(h(y) \| N_i \| SID_i)$

$A_i = h(T_i \| h(y) \| N_i)$

$\text{h}(\text{b} \oplus PW)_i = CID_i \oplus h(T_i \| A_i \| N_i)$

$B_i = h(h(\text{b} \oplus PW) \| h(x \| y))$

$Q_i^{'} = H(B_i \| A_i \| N_i)$

Checks $Q_i^{'} \overset{?}{=} Q_i$, generates N_j

$M_{ij} = h(B_i \| N_i \| A_i \| SID_j)$

$\xleftarrow{(M_{ij}, N_j)}$

$M_{ij}^{'} = h(B_i \| N_i \| A_i \| SID_j)$

Checks $M_i^{'} \overset{?}{=} M_i$

$M_{ij}^{''} = h(B_i \| N_j \| A_i \| SID_j)$

$\xrightarrow{M_{ij}^{''}}$

$M_{ij}^{'''} = h(B_i \| N_j \| A_i \| SID_j)$

Checks $M_i^{'''} \overset{?}{=} M_i^{''}$

$SK = h(B_i \| N_i \| N_j \| A_i \| SID_j)$ $\longleftrightarrow$ $SK = h(B_i \| N_i \| N_j \| A_i \| SID_j)$

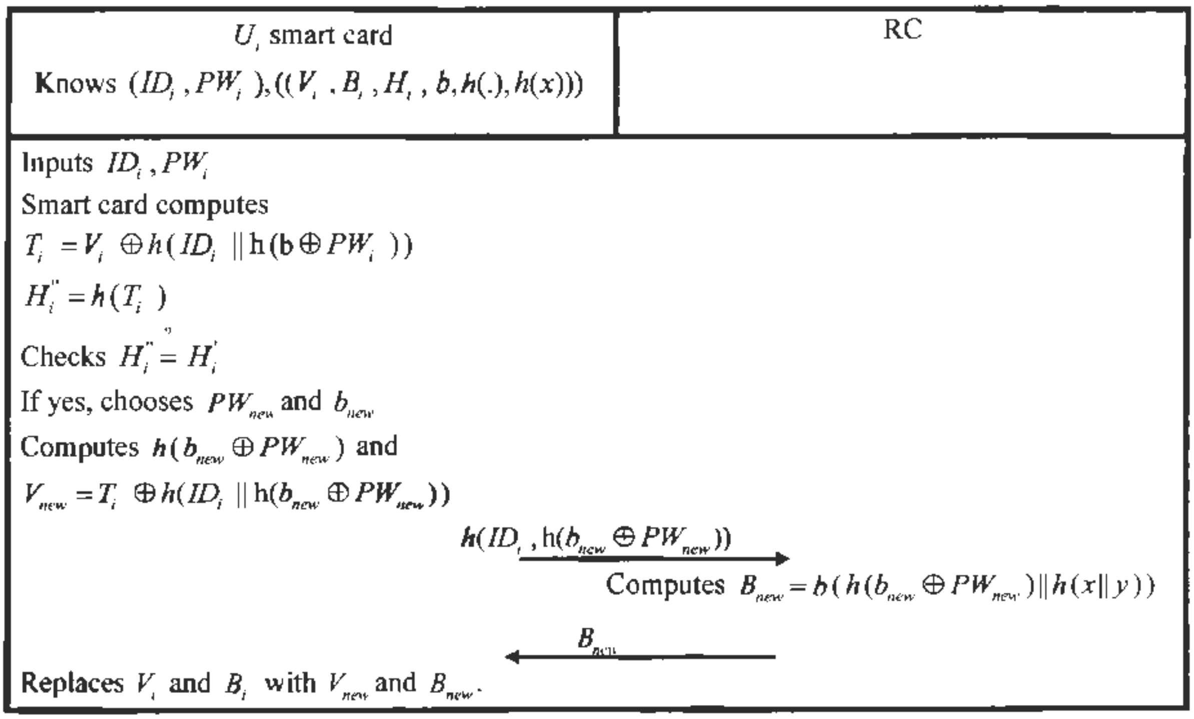
Figure 7: Lee et al.'s scheme's Login and Authentication phase

iv. **Password Change phase:**

The User insert ID_i, PW_i, the SmartCard then computes:

$T_i = V_i \oplus h(ID_i \,||\, \mathrm{h}(\mathrm{b} \oplus PW_i))$
$H_i'' = h(T_i)$

And check $H_i'' \overset{?}{=} H_i'$ if both are equal the user is asked to enter new Password PW_{new} and new random number b_{new} then the smartcard compute $h(b_{new} \oplus PW_{new})$ and $V_{new} = T_i \oplus h(ID_i \,||\, \mathrm{h}(b_{new} \oplus PW_{new}))$, and then send $h(ID_i, \mathrm{h}(b_{new} \oplus PW_{new}))$. The server in receiving $h(ID_i, \mathrm{h}(b_{new} \oplus PW_{new}))$ computes $B_{new} = h(h(b_{new} \oplus PW_{new}) || h(x||y))$ and send B_{new} to the user. The user on receiving B_{new} replaces V_i and B_i with V_{new} and B_{new}.



U_i smart card Knows $(ID_i, PW_i), ((V_i, B_i, H_i, b, h(.), h(x)))$	RC

Inputs ID_i, PW_i
Smart card computes
$T_i = V_i \oplus h(ID_i \,||\, \mathrm{h}(\mathrm{b} \oplus PW_i))$
$H_i'' = h(T_i)$
Checks $H_i'' \overset{?}{=} H_i'$
If yes, chooses PW_{new} and b_{new}
Computes $h(b_{new} \oplus PW_{new})$ and
$V_{new} = T_i \oplus h(ID_i \,||\, \mathrm{h}(b_{new} \oplus PW_{new}))$

$\xrightarrow{h(ID_i,\, \mathrm{h}(b_{new} \oplus PW_{new}))}$

Computes $B_{new} = b(h(b_{new} \oplus PW_{new}) || h(x||y))$

$\xleftarrow{B_{new}}$

Replaces V_i and B_i with V_{new} and B_{new}.

Figure 8: Lee et al.'s scheme's Password Change phase

Limitations:

Lee et al.'s.'s scheme is having the following security issues:

1. Offline Password Guessing attack
2. Server spoofing attack
3. Masquerade attack

2.12. Efficient and Secure Dynamic ID-Based remote user authentication scheme for distributed system using smart cards [26]

In this paper the author proposed a solution to solve the security issues in Lee et al.'s scheme. Like Lee et al.'s scheme the proposed scheme also have three core participants: U_i (user) S_i (Server) and RC. To calculate $h(x\|y)$ and $h(y)$ the RC selects x master secret key and y secret number and then share $h(x\|y)$ and $h(y)$ over the secure channel. The proposed solution is divided into Registration, Login, verification and Password change phases.

i. **Registration phase:**

In this phase the User selects his identity ID_i, Password PW_i and a random number b and then calculate $A_i=h(b\oplus PW_i)$ and then send (ID_i, A_i) to the server. The server on receiving (ID_i, A_i), selects a random number R_i and calculates:

$T_i = h(R_i\|x)$
$Z_i = R_i \oplus ID_i \ominus h(b\oplus PW_i)$
$V_i = T_i \oplus h(ID_i\|h(b\oplus PW_i))$
$B_i = h(b\oplus PW_i)\oplus ID_i \oplus h(h(b\oplus PW_i \oplus R_i)\|h(x\|y))$
$H_i = h(T_i)$

After the computation of above the Server then store $(Z_i, V_i, B_i, H_i, h(\bullet), h(y))$ into a SmartCard and then send SmartCard to the User. The User on receiving SmartCard, store b into the SmartCard.

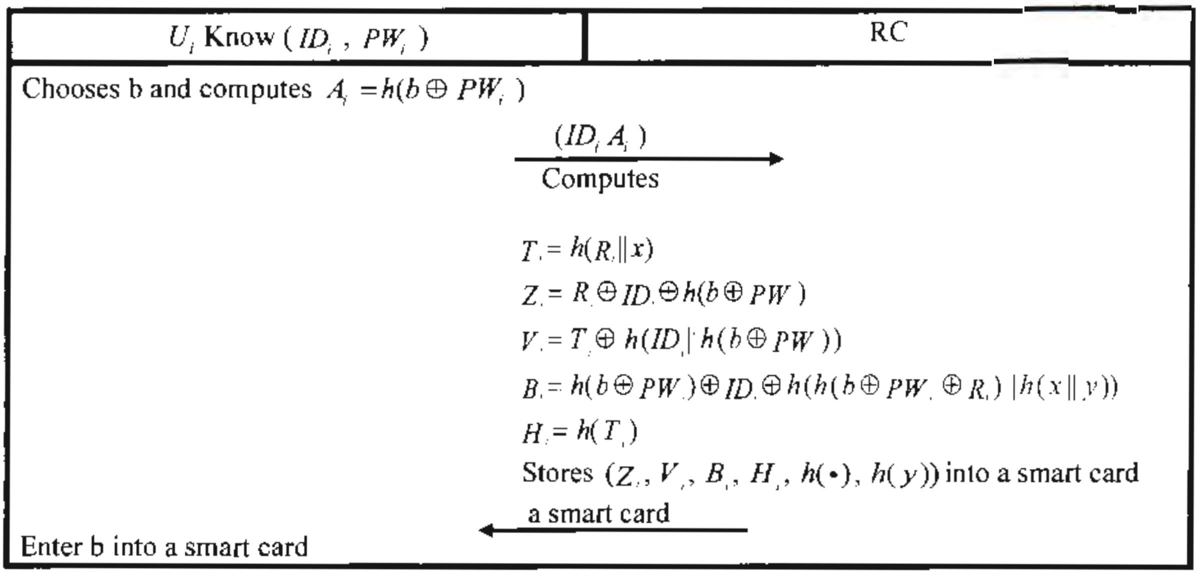

U_i Know (ID_i, PW_i)
RC
Chooses b and computes $A_i = h(b\oplus PW_i)$
$(ID_i A_i)$
Computes
$T_i = h(R_i\|x)$
$Z_i = R_i \ominus ID_i \ominus h(b\oplus PW_i)$
$V_i = T_i \oplus h(ID_i|h(b\oplus PW_i))$
$B_i = h(b\oplus PW_i)\oplus ID_i \oplus h(h(b\oplus PW_i \oplus R_i)|h(x\|y))$
$H_i = h(T_i)$
Stores $(Z_i, V_i, B_i, H_i, h(\bullet), h(y))$ into a smart card
a smart card
Enter b into a smart card

Figure 9: Leu et al.'s scheme's Registration phase

i. Log in Phase:

When the user want to login into the server, the user insert his SmartCard and then insert his id ID_i, password PW_i and the server Identity SID_i. The SmartCard then calculate:

$$R_i = Z_i \oplus ID_i \oplus h(b \oplus PW_i)$$
$$T_i = V_i \oplus h(ID_i \| h(b \oplus PW_i))$$
$$H_i' = h(T_i)$$

And then check $H_i' \overset{?}{=} H_i$, if equal then user U_i is a authorized user. The SmartCard then generate a Random number N_i and calculate:

$$O_i = h(b \oplus PW_i) \oplus ID_i \oplus B_i$$
$$= h(h(b \oplus PW_i \oplus R_i) \| h(x \| y))$$
$$A_i = h(T_i \| h(y) \| N_i)$$
$$CID_i = h(b \oplus PW_i \oplus R_i) \oplus h(T_i \| A_i \| N_i)$$
$$P_{ij} = T_i \oplus h(h(y) \| N_i \| SID_i)$$
$$Q_i = h(O_i \| A_i \| N_i)$$

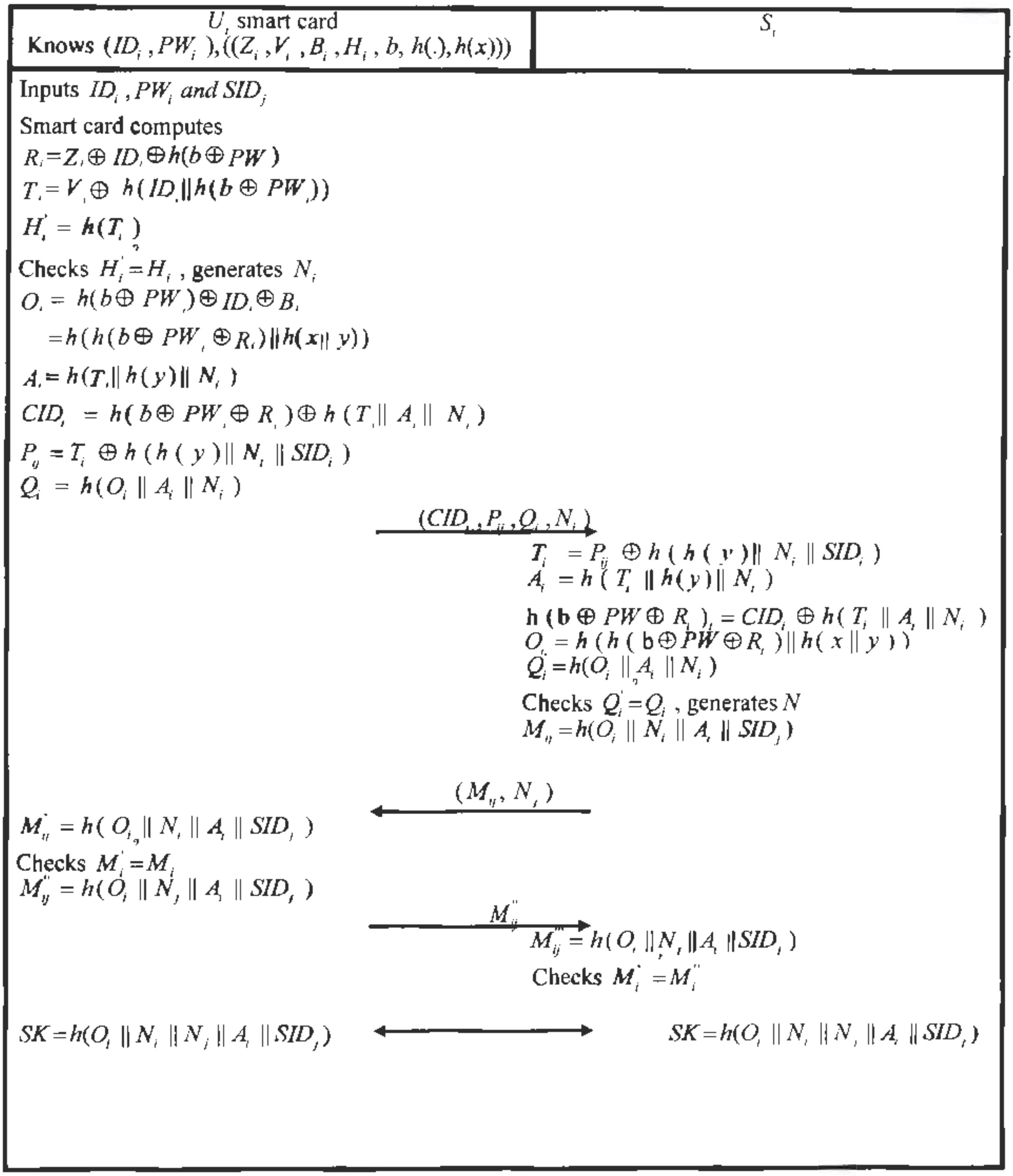
And then send $(CID_i, P_{ij}, Q_i, N_i)$ to the server.

ii. Verification phase:

The server on receiving $(CID_i, P_{ij}, Q_i, N_i)$ calculate:

$$T_i = P_{ij} \oplus h(h(y) \| N_i \| SID_i)$$
$$A_i = h(T_i \| h(y) \| N_i)$$
$$\mathrm{h}(\mathrm{b} \oplus PW \oplus R_i)_i = CID_i \oplus h(T_i \| A_i \| N_i)$$
$$O_i = h(h(\mathrm{b} \oplus PW \oplus R_i) \| h(x \| y))$$
$$Q_i' = h(O_i \| A_i \| N_i)$$

check $Q_i' \overset{?}{=} Q_i$, if both are not equal the server drop the login request otherwise the request is accepted and the server generate random number N_j to compute $M_{ij} = h(O_i \| N_i \| A_i \| SID_j)$ and send (M_{ij}, N_j) to the user. The user on receiving (M_{ij}, N_i) compute $M_{ij}' = h(O_i \| N_i \| A_i \| SID_j)$ and then compare $M_i' \overset{?}{=} M_i$, if both are equal the user compute $M_{ij}'' = h(O_i \| N_j \| A_i \| SID_j)$ and send M_{ij}'' to the server otherwise drop the response. The Server on receiving M_{ij}'' compute $M_{ij}''' = h(O_i \| N_j \| A_i \| SID_j)$ and then compare $M_i''' \overset{?}{=} M_i''$ if both are equal both User and Server share session key $SK = h(O_i \| N_i \| N_j \| A_i \| SID_j)$ for secure communication.



U_i smart card
Knows $(ID_i, PW_i), ((Z_i, V_i, B_i, H_i, b, h(.), h(x)))$

S_i

Inputs ID_i, PW_i *and* SID_j

Smart card computes

$R_i = Z_i \oplus ID_i \oplus h(b \oplus PW)$

$T_i = V_i \oplus h(ID_i \| h(b \oplus PW_i))$

$H_i' = h(T_i)$

Checks $H_i' \overset{?}{=} H_i$, generates N_i

$O_i = h(b \oplus PW_i) \oplus ID_i \oplus B_i$

$= h(h(b \oplus PW_i \oplus R_i) \| h(x \| y))$

$A_i = h(T_i \| h(y) \| N_i)$

$CID_i = h(b \oplus PW_i \oplus R_i) \oplus h(T_i \| A_i \| N_i)$

$P_{ij} = T_i \oplus h(h(y) \| N_i \| SID_i)$

$Q_i = h(O_i \| A_i \| N_i)$

$\xrightarrow{(CID_i, P_{ij}, Q_i, N_i)}$

$T_i = P_{ij} \oplus h(h(y) \| N_i \| SID_i)$

$A_i = h(T_i \| h(y) \| N_i)$

$\mathbf{h}(\mathbf{b} \oplus PW \oplus R_i)_i = CID_i \oplus h(T_i \| A_i \| N_i)$

$O_i = h(h(\mathrm{b} \oplus PW \oplus R_i) \| h(x \| y))$

$Q_i' = h(O_i \| A_i \| N_i)$

Checks $Q_i' \overset{?}{=} Q_i$, generates N

$M_{ij} = h(O_i \| N_i \| A_i \| SID_j)$

$\xleftarrow{(M_{ij}, N_j)}$

$M_{ij}' = h(O_i \| N_i \| A_i \| SID_j)$

Checks $M_i' = M_i$

$M_{ij}'' = h(O_i \| N_j \| A_i \| SID_j)$

$\xrightarrow{M_{ij}''}$

$M_{ij}''' = h(O_i \| N_j \| A_i \| SID_j)$

Checks $M_i' = M_i''$

$SK = h(O_i \| N_i \| N_j \| A_i \| SID_j)$ $\longleftrightarrow$ $SK = h(O_i \| N_i \| N_j \| A_i \| SID_j)$

Figure 10: Leu et al.'s scheme's Login and authentication phase

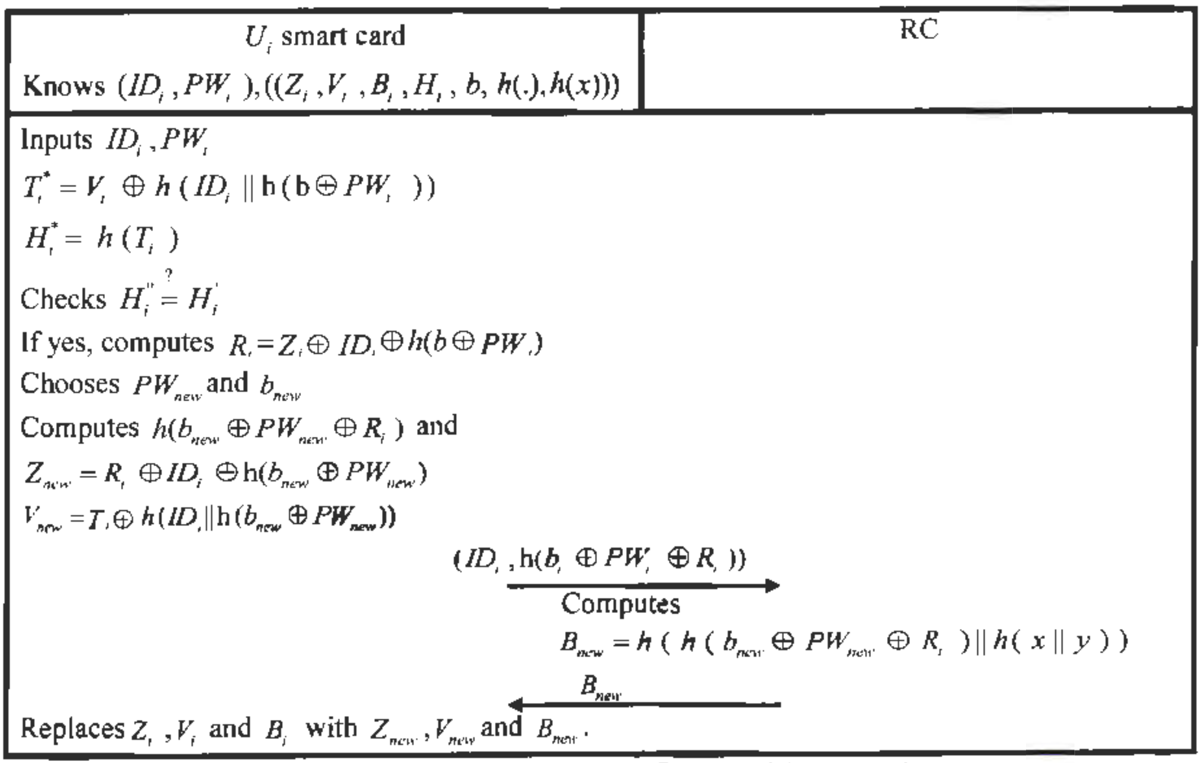
iii. Password Change Phase:

The User insert ID , PW,, the SmartCard then computes:

$T_i^* = V_i \oplus h(ID_i \,||\, \mathrm{h}(\mathrm{b} \oplus PW_i))$
$H_i^* = h(T_i)$

And check $H_i^{''} \overset{?}{=} H_i^{'}$ if both are equal, computes $R_i = Z_i \oplus ID_i \oplus h(b \oplus PW_i)$ and then the user is asked to choose PW_{new} and new random number b_{new} then the smartcard compute $h(b_{new} \oplus PW_{new} \oplus R_i)$ and $Z_{new} = R_i \oplus ID_i \oplus \mathrm{h}(b_{new} \oplus PW_{new})$,and $V_{new} = T_i \oplus h(ID_i \,||\, \mathrm{h}(b_{new} \oplus PW_{new}))$ then the user send $(ID_i, \mathrm{h}(b_i \oplus PW_i \oplus R_i))$.

The server on receiving $(ID_i, \mathrm{h}(b \oplus PW_i \oplus R_i))$ computes $B_{new} = h(h(b_{new} \oplus PW_{new} \oplus R_i) \,||\, h(x \,||\, y))$ and send B_{new} to the user. The user on receiving B_{new} replaces Z_i , V_i and B_i with Z_{new} , V_{new} and B_{new} .



U_i smart card

Knows $(ID_i, PW_i), ((Z_i, V_i, B_i, H_i, b, h(.), h(x)))$

RC

Inputs ID_i, PW_i

$T_i^* = V_i \oplus h(ID_i \,||\, \mathrm{h}(\mathrm{b} \oplus PW_i))$

$H_i^* = h(T_i)$

Checks $H_i^{''} \overset{?}{=} H_i^{'}$

If yes, computes $R_i = Z_i \oplus ID_i \oplus h(b \oplus PW_i)$

Chooses PW_{new} and b_{new}

Computes $h(b_{new} \oplus PW_{new} \oplus R_i)$ and

$Z_{new} = R_i \oplus ID_i \ominus \mathrm{h}(b_{new} \oplus PW_{new})$

$V_{new} = T_i \oplus h(ID_i \,||\, \mathrm{h}(b_{new} \oplus PW_{new}))$

$\xrightarrow{(ID_i, \mathrm{h}(b_i \oplus PW_i \oplus R_i))}$

Computes

$B_{new} = h(h(b_{new} \oplus PW_{new} \oplus R_i) \,||\, h(x \,||\, y))$

$\xleftarrow{B_{new}}$

Replaces Z_i , V_i and B_i with Z_{new} , V_{new} and B_{new} .

Figure 11: Leu et al.'s scheme's Password Change phase

Limitations:

The proposed scheme is having issues in almost every phase. In Registration phase B_i is incorrectly calculated because of $h(h(b \oplus PW_i \oplus R_i)$. In Login and Authentication phase, the user is sending anonymous id CID_i and the original id of the user is not known to the server and hence the server is unable to identify the user. The change phase is incorrect because the user is sending incorrect password $(ID_i$, h$(b_i \oplus PW_i \oplus R_i$)) to the server.

Chapter 3

Proposed Scheme

3. Problem Statement

Existing authentication schemes are based on public key infrastructure (i.e. Elliptic Curve, RSA etc.) are more secure as compared to authentication schemes based on lightweight symmetric primitives like hash, symmetric encryption, XOR etc.

On the other hand symmetric primitives are more lightweight and suitable for resource constraints environment such as TMIS. But such schemes are vulnerable to different attacks, while some of them are having correctness issues.

Notation	Description
S:	Server
ID_i	Identity of U_i
U_i	The legal client
PW_i	Password of the client
x, y	Secret keys of S
$\oplus$	Bitwise XOR operation
CID_i	Pseudo identity of u_i
A	The Adversary
$\|\|$	String concatenation operator
SC_{ui}	u_i smart card
$h(.)$	A one way hash function
SK	Session key

Table 1: Notation Guide

3.1 Proposed Scheme:

Our proposed solution is divided into, Registration, Log in and Authentication and Password Change phases. All the three phases are elaborated as below.

3.1.1 Registration phase: In this phase User u_i , (a legal system user) need to register itself at the server S_i . The Registration is done as follow:

i. Step RP1: $u_i \rightarrow S:\{ID_i, A_i\}$

- User u_i select his id ID_i , Password PW_i and a random number b and then calculates C_i =h(b $\oplus$ PW_i)and then send registration request $\{ID_i, C_i\}$ to the server.

ii. $S \rightarrow u_i : SmartCard\{SC_{ui}\}$

- The server on receiving $\{ID_i, C_i\}$, computes his random number R_i where R_i is unique for every user.
- And then the server computes:

a. $T_i = h(R_i \| x)$.

b. $Z_i = R_i \oplus ID_i \oplus C_i$.

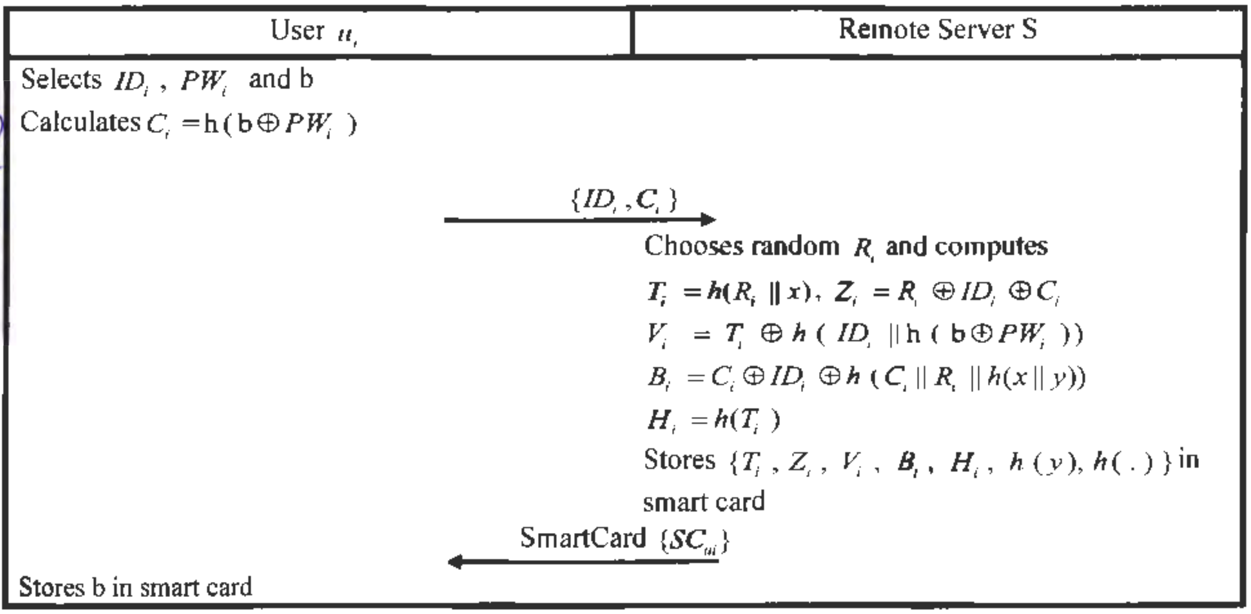
c. $V_i = T_i \oplus h(ID_i \| \mathrm{h}(\mathrm{b} \oplus PW_i))$.

d. $B_i = C_i \oplus ID_i \oplus h(C_i \| R_i \| h(x \| y))$ where y and x are the secret keys of Server S_i.

e. $H_i = h(T_i)$.

- The server then stores $\{T_i, Z_i, V_i, B_i, H_i, h(y), h(.)\}$ in to the smartcard SC_{ui} and send Smartcard $\{SC_{ui}\}$.

iii. On receiving Smartcard $\{SC_{ui}\}$ the User u_i stores its random number b in the SmartCard.



User u_i	Remote Server S
Selects ID_i, PW_i and b Calculates $C_i = \mathrm{h}(\mathrm{b} \oplus PW_i)$	

$\xrightarrow{\{ID_i, C_i\}}$

Chooses random R_i and computes

$T_i = h(R_i \| x)$, $Z_i = R_i \oplus ID_i \oplus C_i$

$V_i = T_i \oplus h(ID_i \| \mathrm{h}(\mathrm{b} \oplus PW_i))$

$B_i = C_i \oplus ID_i \oplus h(C_i \| R_i \| h(x \| y))$

$H_i = h(T_i)$

Stores $\{T_i, Z_i, V_i, B_i, H_i, h(y), h(.)\}$ in smart card

$\xleftarrow{\text{SmartCard } \{SC_{ui}\}}$

Stores b in smart card

Figure 12: Registration phase of our scheme

3.1.2. Login and Authentication phase:

In this phase when a registered user u_i wish to access server S services, he enters his SC into a terminal device and then enter his id ID_i, Password PW_i, and then to compute login request the $\{SC_{ui}\}$ performed the following steps:

i. $u_i \rightarrow S: \{CID_i, P_i, Q_i, N_i\}$

- SC_{ui} computes:

a. $R_i = Z_i \oplus ID_i \oplus h(\mathrm{b} \oplus PW_i)$.

b. $T_i = V_i \oplus h(ID_i \| h(\mathrm{b} \oplus PW_i))$.

c. $H_i^* = h(T_i)$ and then SC_{ui} compare $H_i^* \overset{?}{=} H_i$ SC_{ui} drop the session if $H_i^* \neq H_i$, otherwise compute the following:

d. $O_i = h(\mathrm{b} \oplus PW_i) \oplus ID_i \oplus B_i$.
$= h(\mathrm{b} \oplus PW_i) \| R_i \| h(x \| y))$.

e. $A_i = h(T_i \| h(y \| N_i))$.

f. $CID_i = h(b \oplus PW_i \oplus R_i) \oplus h(T_i \| A_i \| N_i)$.

g. $P_{ij} = T_i \oplus h(x \| y) \| N_i \| SID_j)$.

h. $Q_i = h(O_i \| A_i \| N_i)$.

ii. The SC_{ui} send login request $\{CID_i, P_i, Q_i, N_i\}$ to Server S via public channel.

iii. $S \rightarrow u_i : \{M_{ij}, N_j\}$

- On receiving $\{CID_i, P_i, Q_i, N_i\}$ authentication between the server S_i and user u_i is done by computing:

a. $T_i = P_{ij} \oplus h(h(x) \| N_i \| SID_j)$.

b. $A_i = h(T_i \| h(y) \| N_i)$.

c. $h(b \oplus PW_i \| R_i) = CID_i \oplus h(T_i \| A_i \| N_i)$.

d. $O_i = h(h(b \oplus PW_i \| R_i \| h(x \| y))$.

e. $Q_i^* = h(O_i \| A_i \| N_i)$ and check $Q_i^* \overset{?}{=} Q_i$, the server reject the login request, if $Q_i^* \neq Q_i$ otherwise the server generates random number N_j and computes: $M_{ij} = h(O_i \| N_i \| A_i \| SID_j)$ and then send $\{M_{ij}, N_j\}$ to the user.

iv. $u_i \rightarrow S : PID_i, M_{ij}''$

- On receiving $\{M_{ij}, N_j\}$ the User computes $M_{ij}' = h(O_i \| N_i \| A_i \| SID_j)$ and then check $M_{ij}' \overset{?}{=} M_{ij}$, if $M_{ij}' \neq M_{ij}$ then the session is discarded otherwise the user compute $PID_i = O_i \oplus ID_i$ and $M''_{ij} = h(O_i \parallel N_j \parallel A_i \parallel SID_j)$ and transmit PID_i, M''_{ij} to the server.

User u_i $(ID_i, PW_i), \{T_i, Z_i, V_i, B_i, H_i, h(y), h(.)\}$		Remote Server S $h(x \parallel y), h(y)$
Enter ID_i, PW_i and SID_j SC_{ui} computes $R_i = Z_i \oplus ID_i \oplus h(b \oplus PW_i)$ $T_i = V_i \oplus h(ID_i \parallel h(b \oplus PW_i))$ $H_i^* = h(T_i)$ $H_i^* \overset{?}{=} H_i$ $O_i = h(b \oplus PW_i) \oplus ID_i \oplus B_i$ $= h(b \oplus PW_i) \parallel R_i \parallel h(x \parallel y))$ $A_i = h(T_i \parallel h(y \parallel N_i)$ $CID_i = h(b \oplus PW_i \oplus R_i) \oplus h(T_i \parallel A_i \parallel N_i)$ $P_{ij} = T_i \oplus h(x \parallel y) \parallel N_i \parallel SID_j)$ $Q_i = h(O_i \parallel A_i \parallel N_i)$		
	$\xrightarrow{\{CID_i, P_i, Q_i, N_i\}}$	$T_i = P_{ij} \oplus h(h(x) \parallel N_i \parallel SID_j)$ $A_i = h(T_i \parallel h(y) \parallel N_i)$ $h(b \oplus PW_i \parallel R_i) = CID_i \oplus h(T_i \parallel A_i \parallel N_i)$ $O_i = h(h(b \oplus PW_i \parallel R_i \parallel h(x \parallel y))$ $Q_i^* = h(O_i \parallel A_i \parallel N_i)$ Checks $Q_i^* \overset{?}{=} Q_i$ $M_{ij} = h(O_i \parallel N_i \parallel A_i \parallel SID_j)$
$M'_{ij} = h(O_i \parallel N_i \parallel A_i \parallel SID_j)$ Check $M'_{ij} \overset{?}{=} M_{ij}$ $PID_i = O_i \oplus ID_i$, $M''_{ij} = h(O_i \parallel N_j \parallel A_i \parallel SID_i)$	$\xleftarrow{\{M_{ij}, N_j\}}$	
	$\xrightarrow{PID_i, M''_{ij}}$	$PID_i = O_i \oplus ID_i$ $M'''_{ij} = h(O_i \parallel N_j \parallel A_i \parallel ID_i)$ Check $M''_{ij} = M'''_{ij}$
$SK = h(O_i \parallel N_i \parallel N_j \parallel A_i \parallel SID_j \parallel ID_i)$		$SK = h(O_i \parallel N_i \parallel N_j \parallel A_i \parallel SID_j \parallel ID_i)$

Figure 13: Login and Authentication phase of our scheme

v. On receiving the PID_i , M''_{ij} , the server computers $ID_i = PID_i \oplus O_i$, $M'''_{ij} = h(O_i \| N_j \| A_i \| ID_i)$ and compare $M''_{ij} = M'''_{ij}$ if $M''_{ij} \neq M'''_{ij}$ then the session is discarded otherwise the session key $SK = h(O_i \| N_i \| N_j \| A_i \| SID_j \| ID_i)$ is computed at both User and Server side.

3.1.3 Password change phase:

In this phase when the user u_i want to change his password PW_i to a new one i.e. PW_{new}, in the proposed solution Password change will be done as follows:

i. $u_i \rightarrow S : \{ID_i , h(b_{new} \oplus PW_{i_{new}})\}$

- User u_i insert his smartcard SC_{ui} into the terminal device, enter his ID_i and PW_i , and computes:

  a. $T_i = V_i \oplus h\,(\,ID_i \| h(b \oplus PW_i\,))$

User u_i	Remote Server S
Insert ID_i , PW_i	
$T_i = V_i \oplus h\,(\,ID_i \| h(b \oplus PW_i\,))$	
$H_i = h\,(\,T_i\,)$	
Check $H_i \overset{?}{=} H_i^*$	
$R_i = Z_i \oplus ID_i \oplus h(b \oplus PW_i\,)$	
Chooses PW_{new} and b_{new}	
$h(b \oplus PW_i \| R_i\,)$	
$R_i = Z_i \oplus ID_i \oplus h(\,b_{new} \oplus PW_{new}\,)$	
$T_i = h\,(\,ID_i \| h\,(\,b_{new} \oplus PW_{new}\,)$	
$\xrightarrow{\{(ID_i , h(b_{new} \ominus PW_{i_{new}})\}}$	
	$B_{new} = h(b_{new} \ominus PW_{new}) \oplus ID_i \ominus h\,(h\,(\,b_{new} \ominus PW_{i_{new}}) \| R_{i_{new}} \| h\,(x \| y))$
$\xleftarrow{\{B_{new}\}}$	
Keeps new values $Z_{new}, V_{new}, B_{new}$	

Figure 14: Password change phase of our scheme

b. $H_i = h(T_i)$ and check $H_i \overset{?}{=} H_i^*$, if $H_i \neq H_i^*$, then password change request is discarded, otherwise calculate $R_i = Z_i \oplus ID_i \oplus h(b \oplus PW_i)$ and choose new password PW_{new} and new random number b_{new}.

c. And computes $h(b \oplus PW_i \| R_i), R_i = Z_i \oplus ID_i \oplus h(b_{new} \oplus PW_{new})$, $T_i = h(ID_i \| h(b_{new} \oplus PW_{new})$ and then transmit $\{ID_i, h(b_{new} \oplus PW_{i_{new}})\}$ to the server.

ii. $S \rightarrow u_i : \{B_{new}\}$

- On receiving $\{(ID_i, h(b_{new} \oplus PW_{i_{new}})\}$ the server calculate $B_{new} = h(b_{new} \oplus PW_{new}) \oplus ID_i \oplus h(h(b_{new} \oplus PW_{i_{new}}) \| R_{i_{new}} \| h(x \| y))$ and then send $\{B_{new}\}$ to the user u_i.

iii. The user u_i store $Z_{new}, V_{new}, B_{new}$ on smartcard SC_{ui}.

Chapter 4

Simulation and Performance Analysis

4. Performance and Security Comparison:

We examine and evaluate the proposed scheme by comparing its performance and security with five related schemes, Kumari et al.'s [30] scheme, Zhang et al.'s [29] scheme, Leu et al.'s [27] scheme, Lee et al.'s [26] scheme and Hsiang et al.'s [28] scheme.

4.1. Performance Analysis:

Here we used some notations, t_h represent time efficiency of hash function and $t_\oplus$ represent time efficiency of EXOR operation.

		Proposed Scheme	Kumari et al. scheme	Zhang et al scheme	Leu et al. Scheme	Lee et al. Scheme	Hsiang et al. Scheme
Registration	User	$1t_\oplus + 1t_h$	$2t_\oplus + 1t_h$	$5t_\oplus + 2t_h$	$1t_\oplus + 1t_h$	$1t_\ominus + 1t_h$	$1t_\ominus + 1t_h$
	Server	$5t_\oplus + 4t_h$	$3t_\oplus + 3t_h$	$2t_\oplus + 0$	$7t_\oplus + 5t_h$	$1t_\oplus + 5t_h$	$4t_\oplus + 6t_h$
Login and Authentication	User	$11t_\oplus + 10t_h$	$10t_\oplus + 6t_h$	$11t_\oplus + 2t_h$	$10t_\oplus + 10t_h$	$4t_\oplus + 9t_h$	$6t_\oplus + 9t_h$
	Server	$3t_\oplus + 7t_h$	$3t_\oplus + 5t_h$	$9t_\oplus + 2t_h$	$2t_\oplus + 7t_h$	$2t_\oplus + 6t_h$	$11t_\oplus + 13t_h$
Password Change	User	$6t_\oplus + 6t_h$	$7t_\ominus + 4t_h$	$7t_\oplus + 1t_h$	$10t_\oplus + 6t_h$	$4t_\oplus + 5t_h$	$4t_\oplus + 5t_h$
	Server	$0 + 2t_\oplus$	0	0	$2t_\oplus + 2t_h$	$0 + 1t_h$	$3t_\oplus + 1t_h$
Total of Login and Authentication		$14t_\oplus + 17t_h$	$13t_\oplus + 11t_h$	$20t_\oplus + 4t_h$	$12t_\oplus + 17t_h$	$6t_\oplus + 15t_h$	$17t_\oplus + 22t_h$

Table 2: Performance Analysis Comparison

In Registration phase, at user side our proposed scheme is taking $1t_\oplus + 1t_h$, Kumari et al.'s scheme is taking $2t_\oplus + 1t_h$, Zhang et al.'s scheme is taking $5t_\oplus + 2t_h$, Leu et al.'s, Lee et al,'s and Hsiang et al.'s schemes are taking $1t_\oplus + 1t_h$. At server side our proposed scheme is taking $5t_\oplus + 4t_h$, Kumari et al.'s scheme is taking $3t_\oplus + 3t_h$, Zhang et al.'s scheme is taking $2t_\oplus + 0$, Leu et al.'s scheme is taking $7t_\oplus + 5t_h$, Lee et al.'s scheme is taking $1t_\oplus + 5t_h$ and Hsiang et al.'s scheme are taking $4t_\oplus + 6t_h$. On a whole in Registration phase, our proposed scheme is taking $6t_\oplus + 5t_h$, Kumari et al.'s scheme is taking $5t_\oplus + 4t_h$, Zhang et al.'s scheme is taking $7t_\ominus + 2t_h$, Leu et al.'s is taking $8t_\oplus + 6t_h$, Lee et al.'s is taking $2t_\oplus + 6t_h$, and Hsiang et al.'s schemes are taking $5t_\oplus + 7t_h$.

Chapter 1

Introduction

In Login and Authentication phase on a whole, our scheme is taking $14t_{\oplus}+17t_{h}$, Kumari et al.'s scheme is taking$13t_{\oplus}+11t_{h}$, Zhang et al.'s scheme is taking $20t_{\oplus}+4t_{h}$, Leu at al.'s scheme is taking $20t_{\oplus}+4t_{h}$ and Hsiang et al.'s is taking $17t_{\oplus}+22t_{h}$, whereas Lee et al.'s scheme is taking $6t_{\oplus}+15t_{h}$ Our in term of efficiency is better than Hsiang schemes whereas Kumari et al.'s, Zhang et al.'s and Lee scheme are better than out scheme but Lee et al.'s scheme is exposed to masquerade ,offline password Guessing and server spoofing attacks, Kumari et al.'s scheme is exposed to smart card loss attack and forward secrecy issues and Zhange et al.'s scheme is exposed to DoS attack and user Un-traceability issues. Similarly Leu at al.'s scheme and our scheme is required same computational resources at login and authentication phase but Leu at al.'s scheme is having correctness issues in almost every phase.

In Password change phase, our scheme at user side is taking $6t_{\oplus}+6t_{h}$ Kumari et al.'s scheme is taking$7t_{\oplus}+4t_{h}$, Zhang et al.'s scheme is taking$7t_{\oplus}+1t_{h}$, Leu at al.'s scheme is taking $10t_{\oplus}+6t_{h}$ Lee et al.'s scheme is taking $4t_{\oplus}+5t_{h}$ and Hsiang et al.'s scheme is also taking $4t_{\oplus}+5t_{h}$. Similarly on server side our proposed scheme is taking $0+2t_{\oplus}$, Kumari and Zhang schemes are taking 0 because in their password change phase server is not involved Leu at al.'s scheme is taking$2t_{\oplus}+2t_{h}$and Hsiang et al.'s scheme is taking$3t_{\oplus}+1t_{h}$, whereas Lee et al.'s scheme is taking $0+1t_{h}$.

4.2. Security Analysis:

In this analysis we have shown some security comparison of our proposed solution with Leu et al.'s Scheme [27], Lee et al.'s [26] scheme, Hsiang et al.'s [28] scheme and Zhang et al.'s [29] scheme.

4.2.1. Informal Security Analysis:

Various security defects are enhanced through our proposed solution which others were at risk. Lee et al.'s scheme is exposed to user impersonation, server spoofing, and offline password guessing attacks and also having some correctness problem in Login and Authentication phase. Leu et al.'s scheme doesn't offer proper mutual authentication and also having correctness problem in Registration, Login and Authentication and in Password change phases. Zhang et al.'s scheme is exposed to DoS attack, doesn't offer user un-traceability also vulnerable to user anonymity violation attack. Hsiang et al.'s scheme is exposed to user impersonation, server spoofing attacks, does not provide proper mutual authentication and also having some correctness issues in log in and authentication phase. Kumari et al.'s scheme is exposed to smart card loss attack and also does not provide forward secrecy.

		Schemes					
		Proposed Scheme	Zhang et al.'s scheme	Kumari et al.'s scheme	Leu et al. Scheme	Lee et al.'s Scheme	Hsiang et al.'s scheme
Security characteristics	Resists against insider attack	Yes	Yes	Yes	Yes	Yes	Yes
	Resists against smart card loss attack	Yes	Yes	No	Yes	Yes	Yes
	Resists against user impersonation attack	Yes	Yes	Yes	Yes	No	No
	Resists against server spoofing attack	Yes	Yes	Yes	Yes	No	No
	Resists against offline password guessing	Yes	Yes	Yes	Yes	No	Yes
	Resists against replay attack	Yes	Yes	Yes	Yes	Yes	Yes
	Resists against stolen verifier attack	Yes	Yes	Yes	Yes	Yes	Yes
	Resists against DoS attack	Yes	No	Yes	Yes	Yes	Yes
	Provides forward secrecy	Yes	Yes	No	Yes	Yes	Yes
	Provides user un-traceability	Yes	No	Yes	Yes	Ycs	Yes
	Provides proper mutual authentication	Yes	Yes	Yes	No	Yes	No
	Provide anonymity	Yes	No	Yes	Yes	Yes	Yes
	Correctness of Registration phase	Yes	Yes	Yes	No	Yes	Yes
	Correctness of Login and Authentication phase	Yes	Yes	Yes	No	No	No
	Correctness of Password Change Phase	Yes	Yes	Yes	No	Yes	Yes

Table 3: Informal Security Comparison

4.2.2. Security proof using Automated tool ProVerif:

ProVerif is widely used for observing the safety of Cryptographic procedure. Cryptographic safety support includes, symmetric key and public key encryption, one way hash functions, elliptic curve etc. Proverif is able to prove observational-equivalence, correspondence assertions, and reachability properties. These abilities are mainly beneficial to computer security areas like authentication, privacy, verifiability and traceability etc. Proverif is such a strong tool, if a protocol is found as insecure then it is insecure in real environment as well.

ProVerif has been established on OCaml (Objective Caml) and is based on pi calculus. Pi-calculus is known as process calculus and is used for processes interconnection i.e. they can transmit and obtain messages on channels. In Pi-Calculus channels and messages are names having atomic value x, y, x....

- **Declaration in ProVerif:**

Procedures are having limited set of types, free names, constructors and destructors etc. In Proverif syntax of user define type is:

```
type t.
```

Free names are declared as:

```
free n : t.
```

where n represent the name and t represent the type of name n. Free names are by default recognized by the opponent and to keep the Free name secret, those Free names should be declared as private.

```
free n : t [private].
```

free c : channel is a syntax for declaring a channel with name c.

- **Defining channels:**

We define two channels, secure channel for Registration and Insecure channel Log in and authentication.

```
(* ------------channels--------------*)
free schuts:channel  [private]. (*Secure*).
free ichuts:channel. (*InSecure*).
```

- **Defining Constant:**

We define bitsting private constants and bitsting public constants which we will use later in the implementation. Where iPW represent password of the user and IDi represent id of the user. SIDj represent id of the server, x and y are the private keys of server.

```
(*-------------constants----------------*)
const iPW:bitstring  [private].
const x:bitstring  [private].
const y:bitstring  [private].
const IDi: bitstring .
const SIDj: bitstring .
```

- **Defining constructor:**

To construct terms modelling basics for cryptographic-protocols Constructor/functions are used. Constructor can be define as:

$fun\, f(t_1...t_n):t$ Where f represent a constructor with n arity, $t_1...t_n$ represents the argument types and t is the return type.

We define following functions/constructors which accept bitstring and will return bitstring, hash(bitstring) is the Hash functions, concat(bitstring,bitstring) is the concatenation function which will concatenate two bitstrings, fun Exor(bitstring,bitstring) is the EXOR function and Symenc(bitstring,bitstring) function is used for Symmetric encryption and the return value will be keep private by user and server.

```
(*---------------constructor----------------*)
fun hash (bitstring): bitstring.
fun concat (bitstring, bitstring): bitstring.
fun Exor (bitstring, bitstring): bitstring.
fun Symenc (bitstring, bitstring): bitstring  [private].
```

- **Defining Destructors and Equations:**

Destructor is the inverse function of constructor and is used to control terms made/configured by constructor. Destructor can be defined as:

reduc for all $\mathrm{x}_{1,1} : t_{1,1}$, x_{1,n_1} : t_{1,n_1} : $g(\mathrm{M}_{1,1},...M_{1,k}) = M_{1,0}$;

....

reduc for all $\mathrm{x}_{m,1} : t_{m,1}$, x_{m,n_m} : t_{m,n_m} : $g(\mathrm{M}_{m,1},...M_{m,k}) = M_{m,0}$;

Where g represents destructor of arity k, $\mathrm{M}_{1,1},...M_{1,k}$ are created by constructor using variables, $\mathrm{x}_{1,1},...x_{1,n_1}$ of type $\mathrm{t}_{1,1},...t_{1,n_1}$.

Destructors and equations are define for inverse functions, we used destructor for inverse of Symenc functions and equation is used for inverse of Exor functions.

"Symdec(Symenc(m,key),key)=m" destructor is used for message decryption which is the inverse function of Symenc function. "Exor(Exor(a,b),b)=a." is the inverse equation of of Exor function.

```
(*---------------destructors & equations-----------------*)
reduc forall m: bitstring,key: bitstring;  Symdec (Symenc(m,key), key)=m.
equation forall a: bitstring, b: bitstring; Exor(Exor(a,b), b)=a.
```

- **Defining Events:**

Events are used to verify that the process is started and end by the same user or same server or not.

Event beginiUser(bitstring) is the user start event and event endiUser(bitstring) is the user end event. Similarly event beginReServer(bitstring) is the server start event and event endReServer(bitstring) is the server end event. Whenever user starts process user start event must be trigger first and whenever user process ends, the user end event will be triggered which will indicate that whether the process start and process end user is the same or not. Same is the case for Server, whenever server start process, server start event will be triggered and server end event will be triggered whenever the server end the process.

```
(*------------------------events---------------------------*)
event beginiUser(bitstring).
event endiUser(bitstring).
event beginReServer(bitstring).
event endReServer(bitstring).
```

- **Defining query:**

Here we first define session key sk and then launch attack "query attacker(sk)" on that key . The user query "query id: bitstring; inj-event(endiUser (id)) ==> inj-event(beginiUser(id))" states that this query is true if and only if , for all the execution of the protocol if the event "endiUser(id)" is executed then the event "beginiUser(id)" has also been executed. Similar is the case for server side event "query id: bitstring; inj-event (endReServer(id)) ==> inj-event(beginReServer(id))".

```
(*-----------------------query------------------------------*)
free sk: bitstring  [private].
query attacker (sk).
query id: bitstring; inj-event(endiUser(id)) ==> inj-event(beginiUser(id)) .
query id: bitstring; inj-event(endReServer(id)) ==> inj-event(beginReServer(id)) .
```

- **User's side and Server's Registration Process:**

In the registration process we first define a User "let pUseri=" then we define id for the user "new IDi:bitstring", then we define a random number b "new b:bitstring". The user then Calculate Ci "let Ci=hash(Exor(b,iPW)) in" and then send the (IDi,Ci) to the server on a secure channel "out(schuts,(IDi,Ci))", here "out" keyword is used for sending and "in" keyword is user for receiving. The user received xZi,xVi,xBi,xHi,xhy from server on secure channel.

```
(*--------------------- User's Registration Process--------------------------*)
let pUseri=
new IDi:bitstring;
new b:bitstring;
let Ci=hash(Exor(b,iPW)) in
out(schuts,(IDi,Ci));
in(schuts,(xZi:bitstring,xVi:bitstring,xBi:bitstring,xHi:bitstring,xhy:bitstring));
```

Similarly we define server "let pServeri=" then we define random number Ri "new Ri:bitstring". The server received (IDi,Ci) from the user "in(schuts,(xIDi:bitstring,xCi:bitstring))" and then calculate Ti, Zi, Vi, Bi and Hi. Then the server transmit (Zi,Vi,Bi,Hi,hash(y)) on private channel "out(schuts,(Zi,Vi,Bi,Hi,hash(y)))".

```
(*--------------------- Server's Registration processes-------------------------*)
let pServeri=
new Ri:bitstring;
in(schuts,(xIDi:bitstring,xCi:bitstring));
let Ti=hash(concat(Ri,x)) in
let Zi=Exor(Ri,Exor(IDi,xCi)) in
let Vi=Exor(Ti,hash(concat(IDi,xCi))) in
let Bi=Exor(xCi,Exor(IDi,hash(concat(Ri,hash(concat(x,y)))))) in
let Hi=hash(Ti) in
out(schuts,(Zi,Vi,Bi,Hi,hash(y))) ;
```

- **User's and Server's Login and Authentication Process:**

Here we first triggered the start event of the user "beginiUser(IDi)". Then we calculate Ri, Ti, inverse of Hi' (inverse of Hi) then we select a random number Ni and then compare Hi' and Hi "if(Hi'=xHi)" if both are equal then calculate Oi, Ai, Ai, CIDi, Pij, Qi and then send (CIDi,Pij,Qi,Ni) on insecure channel to the server "out(ichuts,(CIDi,Pij,Qi,Ni))".

Then user then received (Mij,XNj)on insecure channel "in(ichuts,(XMij:bitstring,XNj:bitstring))". On receiving (Mij, Nj) the user then calculate Mij' and then compare Mij' and XMij, if both are equal then calculate Mij" and send Mij" to the server on insecure channel. The user's end event is then triggered "event endiUser(IDi)".

```
(*------------------------User's side Login and Authentication Process-------------------------
-*)
event beginiUser(IDi);
let Ri= Exor(Zi,Exor(IDi,Ci)) in
let Ti= Exor(xVi,hash(concat(IDi,Ci))) in
let Hi'=hash(Ti) in
new Ni:bitstring;
if(Hi'=xHi)
let Oi=Exor(Ci,Exor(IDi,xBi)) in
let Ai=hash(concat(Ti,concat(xhy,Ni))) in
let CIDi=Exor(hash(Exor(b,Exor(iPW,Ri))),hash(concat(Ti,concat(Ai,Ni)))) in
let Pij=Exor(Ti,hash(concat(xhy,concat(Ni,SIDj)))) in
let Qi=hash(concat(Oi,concat(Ai)))
out(ichuts,(CIDi,Pij,Qi,Ni));
in(ichuts,(XMij:bitstring,XNj:bitstring));
let Mij' = hash(concat(Oi,concat(Ni,concat(Ai,SIDj)))) in
if(Mij' = XMij) then
let Mij" = hash(concat(Oi,concat(XNj,concat(Ai,SIDj)))) in
out(ichuts,(Mij"));
event endiUser(IDi).
```

Similarly on server side first Server start event is triggered "event beginReServer(xIDi)". The server on receiving (CIDi,Pij,Qi,Ni) from the user, calculate Ti' (invser of Ti), Ai, xy, Oi, Qi' and then compare Oi and Qi' "if(Qi' = XQi) then". If both are equal then select a random number Nj then calculate Mij and send ,(Mij,Nj) to the user on insecure channel. (a,Ts2,Zi) to the user on private channel.

On receiving Mij" from the user on insecure channel the server calculate Mij''' and then compare Mij''' and Mij" "if(XMij"=Mij''') then". If both are equal then calculate a session key Sk and the authentication is completed. The server then triggered end event "event endReServer(xIDi).

```
(*-----------------------Server's Login and Authentication Process--------------------------*)
event beginReServer(xIDi);
in(ichuts,(XCIDi:bitstring,XPij:bitstring,XQi:bitstring,XNi:bitstring));
let Ti'=Exor(XPij,hash(concat(hash(y),concat(XNi,SIDj)))) in
let Ai = hash(concat(Ti,concat(hash(y),XNi))) in
let xy = Exor(XCIDi,hash(concat(Ti,concat(Ai,XNi)))) in
let Oi = hash(concat(xy,hash(concat(x,y)))) in
let Qi' = hash(concat(Oi,concat(Ai,XNi))) in
if(Qi' = XQi) then
new Nj:bitstring;
let Mij = hash(concat(Oi,concat(XNi,concat(Ai,SIDj)))) in
out(ichuts,(Mij,Nj));
in(ichuts,(XMij'':bitstring));
let Mij''' = hash(concat(Oi,concat(Nj,concat(Ai,SIDj)))) in
if(XMij''=Mij''') then
let Sk = hash(concat(Oi,concat(XNi,concat(Nj,concat(Ai,SIDj))))) in
event endReServer(xIDi).
```

The Secrecy of the user and server is demonstrated as follow

```
process ((!pUseri) | (!pServeri))
```

4.2.2.1. Security Results:

- **Result 1:**

```
-- Query inj-event(endReServer(id)) ==> inj-event(beginReServer(id))

    Completing...
    200 rules inserted. The rule base contains 197 rules. 24 rules in the queue.
    400 rules inserted. The rule base contains 365 rules. 11 rules in the queue.
    Starting query inj-event(endReServer(id)) ==> inj-event(beginReServer(id))
    RESULT inj-event(endReServer(id)) ==> inj-event(beginReServer(id)) is true.
```

This result states that the server event is started and ended successfully. Therefore, server reachability is satisfied.

- **Result 2:**

```
-- Query inj-event(endiUser(id_8404)) ==> inj-event(beginiUser(id_8404))
```

```
Completing...

200 rules inserted. The rule base contains 198 rules. 26 rules in the queue.

400 rules inserted. The rule base contains 365 rules. 11 rules in the queue.

Starting query inj-event(endiUser(id_8404)) ==> inj-event(beginiUser(id_8404))

RESULT inj-event(endiUser(id_8404)) ==> inj-event(beginiUser(id_8404)) is true.
```

This result states that the user event is started and ended successfully. Therefore, user reachability is satisfied.

Result 3:

```
-- Query not attacker(sk[])

Completing...

200 rules inserted. The rule base contains 197 rules. 23 rules in the queue.

400 rules inserted. The rule base contains 357 rules. 5 rules in the queue.

Starting query not attacker(sk[])

RESULT not attacker(sk[]) is true.
```

This result satisfied the security of session key, it states that the session key is not vulnerable to any adversary and is only known to the user and server.

Chapter 5

Conclusion

Conclusion:

In this thesis a lightweight authentication scheme for WBASN is proposed. This scheme is comprised of three phases and provides robust security feature. This scheme is specifically designed to mitigate the security flaws and to provide mutual authentication that existing schemes were unable to offer. Furthermore, an ample performance and security assessment is performed in order to scrutinize the efficiency of the proposed scheme against existing schemes. The performance comparison shows that the proposed scheme is lightweight to provide enough security against well-known security attacks and sustains appropriate computational and communication efficiency. In future, we will work on a three factors (Bio Metric, Password and Smart card) authentication scheme.

References

References

[1] Khan, Jamil Y., Mehmet R. Yuce, and Farbood Karami. "Performance evaluation of a wireless body area sensor network for remote patient monitoring." 30th IEEE Annual International Conference of the Engineering in Medicine and Biology Society, pp 1266-1269, 2008.

[2] Mana, Mohammed, Mohammed Feham, and Boucif Amar Bensaber. "Trust Key Management Scheme for Wireless Body Area Networks." International Journal of Network Security Vol. 12 No 2, pp 75-83, 2011.

[3] Keoh, Sye Loong, Emil Lupu, and Morris Sloman. "Securing body sensor networks: Sensor association and key management." IEEE International Conference on Pervasive Computing and Communications, pp 1-6, 2009.

[4] Latre, Benoit, Bart Braem, Ingrid Moerman, Chris Blondia, Elisabeth Reusens, Wout Joseph, and Piet Demeester. "A low-delay protocol for multihop wireless body area networks." Fourth Annual International Conference on Mobile and Ubiquitous Systems: Networking & Services, pp. 1-8, 2007.

[5] Hanson, Mark A., Harry C. Powell Jr, Adam T. Barth, Kyle Ringgenberg, Benton H. Calhoun, James H. Aylor, and John Lach. "Body area sensor networks: Challenges and opportunities." IEEE Computer Society pp 58-65, 2009.

[6] Poon, Carmen CY, Yuan-Ting Zhang, and Shu-Di Bao. "A novel biometrics method to secure wireless body area sensor nctworks for telemedicine and m-health." IEEE Communications Magazine, Vol. 44, No 4, pp 73-81, 2006.

[7] Saleem, Shahnaz, Sana Ullah, and Hyeong Seon Yoo. "On the Security Issues in Wireless Body Area Networks." International Journal of Digital Content Technology and its Applications Vol. 3, No 3, pp 178-184 2009

[8] Ren, Hongliang, Max QH Meng, and Xijun Chen. "Physiological information acquisition through wireless biomedical sensor networks." IEEE International Conference on Information Acquisition, pp 483-488, 2005.

[9] Schwiebert, Loren, Sandeep KS Gupta, and Jennifer Weinmann. "Research challenges in wireless networks of biomedical sensors." Proceedings of the 7th annual international conference on Mobile computing and networking. pp 151-165, 2001.

[10] Brunelli, Davide, Elisabetta Farella, Laura Rocchi, Marco Dozza, Lorenzo Chiari, and Luca Benini."Bio-feedback system for rehabilitation based on a wireless body area

network." Fourth IEEE Annual International Conference on Pervasive Computing and Communications Workshops. pp 531-535, 2006.

[11] Venkatasubramanian, Krishna K., Ayan Banerjee, and Sandeep Kumar S. Gupta. "PSKA: usable and secure key agreement scheme for body area networks." IEEE Transactions on Information Technology in Biomedicine, Vol. 14, No 1, pp 60-68, 2010.

[12] Otto, Chris, Aleksandar Milenkovic, Corey Sanders, and Emil Jovanov. "System architecture of a wireless body area sensor network for ubiquitous health monitoring." Journal of Mobile Multimedia, Vol. 1, No 4, pp 307-326, 2006.

[13] Ye, Wei, John Heidemann, and Deborah Estrin. "An energy-efficient MAC protocol for wireless sensor networks." Twenty-First IEEE Annual Joint Conference of the Computer and Communications Societies, Vol. 3, pp 1567-1576, 2002.

[14] Omeni, Okundu, et al. "Energy efficient medium access protocol for wireless medical body area sensor networks." IEEE Transactions on Biomedical Circuits and Systems. Vol. 2, No 4, pp 251-259, 2008.

[15] Dai, Lillian, Prithwish Basu. and Jason Redi. "An energy efficient and accurate slot synchronization scheme for wireless sensor networks." 3rd IEEE International Conference on Broadband Communications, Networks and Systems, pp 1-8, 2006.

[16] Ng, H. S., M. L. Sim, and C. M. Tan. "Security issues of wireless sensor networks in healthcare applications." BT Technology Journal, Vol. 24 No 2, pp 138-144, 2006.

[17] Warren, S., Lebak, J., Yao, J., Creekmore, J., Milenkovic, A., & Jovanov, E. "Interoperability and security in wireless body area network infrastructures." 27th IEEE Annual International Conference of the Engineering in Medicine and Biology Society, pp 3837-3840, 2005.

[18] Venkatasubramanian, Krishna K., and Sandeep KS Gupta. "Physiological value-based efficient usable security solutions for body sensor networks." ACM Transactions on Sensor Networks Vol. 6, No 4, pp 1-31- 2010.

[19] Yun, D., Kang, J., Kim, J. E., & Kim, D. "A body sensor network platform with two-level communications." IEEE International Symposium on Consumer Electronics, pp 1-6, 2007.

[20] Keoh, Sye Loong. "Efficient group key management and authentication for body sensor networks." IEEE International Conference on Communications, pp 1-6, 2011.

[21] Zhao, Zhenguo. "An efficient anonymous authentication scheme for wireless body area networks using elliptic curve cryptosystem." Journal of medical systems Vol. 38, No 2, pp 1-7, 2014.

[22] Aftab Ali, Sarah Irum, Firdous Kausar, and Farrukh Aslam Khan. "A cluster-based key agreement scheme using keyed hashing for Body Area Networks." Multimedia tools and applications Vol. 66, No 2, pp 201-214, 2013.

[23] Daojing He, Shing-Chow Chan, Yan Zhang, and Haomiao Yang. "Lightweight and Confidential Data Discovery and Dissemination for Wireless Body Area Networks." IEEE Journal of Biomedical and Health Informatics, Vol. 18 No 2, pp 440-448, 2014.

[24] Al Ameen, Moshaddique, Jingwei Liu, and Kyungsup Kwak. "Security and privacy issues in wireless sensor networks for healthcare applications." Journal of medical systems, Vol. 36, No 1, pp 93-101, 2012.

[25] Lee, Cheng-Chi, Tsung-Hung Lin, and Rui-Xiang Chang. "A secure dynamic ID based remote user authentication scheme for multi-server environment using smart cards." Expert Systems with Applications, Vol. 38, No 11, pp 13863-13670, 2011.

[26] Leu, Jenq-Shiou, and Wen-Bin Hsieh. "Efficient and secure dynamic ID-based remote user authentication scheme for distributed systems using smart cards." IET Information Security, Vol. 8, No 2, pp 104-113, 2014.

[27] Hsiang, Han-Cheng, and Wei-Kuan Shih. "Improvement of the secure dynamic ID based remote user authentication scheme for multi-server environment." Computer Standards & Interfaces, Vol. 31, No 6, pp 1118-1123, 2009.

[28] Zhang, Liping, Shanyu Tang, and Shaohui Zhu. "A lightweight privacy preserving authenticated key agreement protocol for SIP-based VoIP." Peer-to-Peer Networking and Applications, pp 1-19, 2014.

[29] Kumari, Saru, Muhammad Khurram Khan, and Xiong Li. "An improved remote user authentication scheme with key agreement." Computers & Electrical Engineering, Vol. 40, No 6, pp 1997-2012, 2014.

[30] Chen, Chi-Tung, and Cheng-Chi Lee. "A two-factor authentication scheme with anonymity for multi-server environments." Security and Communication Networks, Vol. 8, No 8, pp 1608-1625, 2014.

[31] Kumari, Saru, Muhammad Khurram Khan, Xiong Li, and Fan Wu. "Design of a user anonymous password authentication scheme without smart card." International Journal of Communication Systems, DOI. 10.1002/dac.2853, 2014.

[32] Xie, Qi, Na Dong, Duncan S. Wong, and Bin Hu. "Cryptanalysis and security enhancement of a robust two-factor authentication and key agreement protocol." International Journal of Communication Systems, DOI. 10.1002/dac.2858, 2014.