Privacy Protection for the Vulnerabilities in Active Networks

Jaegu Song and Prof. Seok-soo Kim

Hannam University, Department of Multimedia Engineering, 306 791
bhas9@paran.com, wolfpack@hannam.ac.kr

Abstract

Active Networks architecture is composed of execution environment. This differs from the traditional network architecture which seeks robustness and stability by attempting to remove complexity and the ability to change its fundamental operation from underlying network component. Active networking allows the possibility of highly tailored and rapid "real-time" changes to the underlying network operation. This paper proposed an efficient dual authentication key exchanged in an active network scenario. The proposed system does not require the public key cryptography like Diffie-Hellman and RSA and certificates. The scheme protects personal privacy of identity information. It also provides an effective method to protect against DOS attacks with the scope information of initiator's random number table sent by the responder.

Keywords: *Active Networks, Security, Identity Management System*

1. Introduction

In current generation information society has been governed by a collection of huge amounts of information and services that provides convenience to people. However, IMS (Identity Management Systems) have been crucial as the information society is getting bigger. IMS provides a description of the infrastructure within one or between several organizations that have agreed upon a mutual model of trust in managing and using identities. Identity management or ID management is a broad administrative area that deals with identifying individuals in a system (such as a country, a network or an organization) and controlling the access to the resources in that system by placing restrictions on the established identities.

Identity management is multidisciplinary and covers many dimensions such as:

Technical. With identity management systems (identification, implementation, administration and termination of identities with access to information systems, buildings and data within an organization). [1]

Legal. Such as legislation for data protection.

Police. For instance for dealing with identity theft.

Social and humanity. Dealing with issues such as privacy.

Security. With elements such as access control.

Organizations.

In the real-world context of engineering online systems, identity management can involve three perspectives:

A general model of identity can be constructed from a small set of axiomatic principles, for example that all identities in a given abstract namespace are unique and distinctive, or that such identities bear a specific relationship to corresponding entities in the real world. An axiomatic model of this kind can be considered to express "pure identity" in the sense that the model is not constrained by the context in which it is applied.

In general, an entity can have multiple identities, and each identity can consist of multiple attributes or identifiers, some of which are shared and some of which are unique within a given name space. The Figure1 below illustrates the conceptual relationship between identities and the entities they represent, as well as between identities and the attributes they consist of.

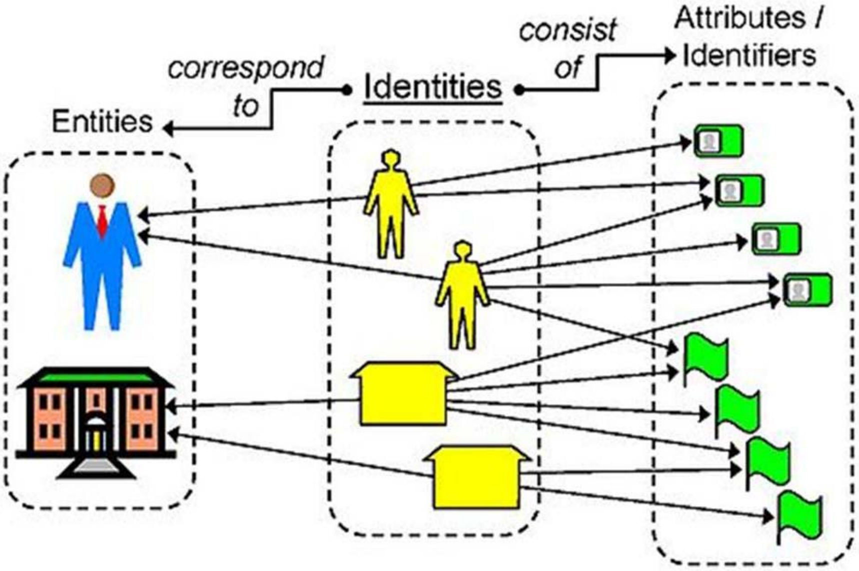

Figure 1. Conceptualize relationship in pure identity [5]

In most theoretical and all practical models of digital identity, a given identity object consists of a finite set of properties. These properties may be used to record information about the object, either for purposes external to the model itself or so as to assist the model operationally, for example in classification and retrieval. A "pure identity" model is strictly not concerned with the external semantics of these properties.

The most common departure from "pure identity" in practice occurs with properties intended to assure some aspect of identity, for example a digital signature or software token which the model may use internally to verify some aspect of the identity in satisfaction of an external purpose. To the extent that the model attempts to express these semantics internally, it is not a pure model.

Contrast this situation with properties which might be externally used for purposes of information security such as managing access or entitlement, but which are simply stored and retrieved, in other words not treated specially by the model. The absence of external semantics within the model qualifies it as a "pure identity" model.

Identity management, then, can be defined as a set of operations on a given identity model, or as a set of capabilities with reference to it. In practice, identity management is often used to express how identity information is to be provisioned and reconciled between multiple identity models.

Another Identity management in the user "log-on" perspective may involve an integrated system of business processes, policies and technologies that enable organizations to facilitate and control access by their users to critical online applications and resources — while protecting confidential personal and business information from unauthorized access. It represents a category of interrelated solutions which system administrators employ towards managing user authentication, Access rights and restrictions, account profiles, passwords, and other attributes supportive of the roles/profiles of user in relation to applications and/or systems. Organizations have traditionally been less concerned with how users can verify the identity of service providers. The emergence of phishing attacks demonstrated that this must be considered as an integral part of the user access paradigm, otherwise users can not know which services they access. Petname systems have been proposed as a general approach to providing service provider identity management solutions.

In the service paradigm perspective, where organizations evolve their systems to the world of converged services, the scope of identity management becomes much larger, and its application more critical. The scope of identity management includes all the resources of the company deployed to deliver online services. These may include devices, network equipment, servers, portals, content, applications and/or products as well as a user's credentials, address books, preferences, entitlements and telephone numbers. See Service Delivery Platform and Directory service.

Today [update], many organizations face a major clean-up in their systems if they are to bring identity coherence into their influence. Such coherence has become a prerequisite for delivering unified services to very large numbers of users on demand — cheaply, with security and single-customer viewing facilities.

The Diffie-Hellman key exchange scheme makes use of difficulty in computing discrete logarithms over a finite field. Since this scheme does not authenticate the participants while exchanging messages, it is vulnerable to man-in-the-middle attacks. For this reason, various authenticated key exchange schemes based on the Diffie-Hellman have been studied by many researchers [10, 11, 12]. These schemes can be categorized into two kinds of classes. The first class employs ‘certificates’ in its key exchange protocol, which foil man-in-the-middle attacks. Certificate-based schemes require additional cost and complexity in key exchange that they are not widely accepted in the market.

The other class proposes its authenticated key exchange protocol with an assumption that a pre-shared secret password or a secret key exists between two communication parties. Most of these authenticated key exchange schemes are not efficient because they use a public key cryptography mechanism which requires high computing power. Recently proposed ones like the IKE [2, 8] consider privacy of personal identity and DOS attacks, which require much more computing power. Recently, mobile computing environment requires low computing power and small memory space even for security service. That is, authenticated key exchange schemes that do not use certificates and public key cryptography are preferable to the mobile environment. This paper proposes an efficient authentication and key exchange scheme that does not use certificates and public key cryptography, while protecting against man-in-the-middle attacks, replay attacks, DOS attacks and privacy intrusion. Characteristics of our scheme are as follows. First, it uses a symmetric block cipher with using a one-way hash function, but without using certificates for dual authentication and key exchange. Since symmetric block cipher requires smaller computing amount and memory space, our scheme is more adaptable to modern distribution environment, such as in ubiquitous and mobile computing. Next, due to the authentication key's one-time property used at each session, our scheme can detect various attacks, such as DOS attacks and man-in-the-middle attacks, without severe computing and memory overhead which overcomes the weakness of Diffie-Hellman. In addition, it solves the problem of identity privacy as well as perfect forward secrecy for future data confidentiality.

However, there is a pressing issue surmounting the IMS, the problem of privacy on the identity management system. Uncertainty about privacy keeps a lot of users away from utilizing IMS. This IMS is always entailed with communication which is the primary concern of this paper particularly the wireless communication since most IMS are already geared to wireless communication. There are challenges in the communication process, many difficulties may occur in the vulnerability reporting process.

Wireless Internet networks security has become a primary concern in order to provide protected communication between mobile nodes in a hostile environment. Unlike the wire-line networks, the unique characteristics of wireless Internet networks pose a number of nontrivial challenges to security design, such as open peer-to-peer network architecture, shared wireless medium, stringent resource constraints, and highly dynamic network topology. These challenges clearly make a case for building multi-fence security solutions that achieve both broad protection and desirable network performance. The unreliability of wireless links between nodes, constantly changing topology due to the movement of nodes in and out of the networks, and lack of incorporation of security features in statically configured wireless routing protocols not meant for wireless Internet environments all lead to increased vulnerability and exposure to attacks. Security in wireless Internet networks is particularly difficult to achieve, notably because of the limited physical protection of each node, the sporadic nature of connectivity, the absence of a certification authority, and the lack of a centralized monitoring or management unit [2][3]

2. Related Works

2.1 P-SIGMA Based Key Exchange Method Using Signal

As a derivation of P-SIGMA, this method uses signals for authenticating users and exchanging keys that are used in symmetric cipher methods. The perfect forward secrecy of One-time-ID can be realized by using the shared secret information which is generated through the Diffie-Hellman key exchange mechanism instead of using a secret key used in P-SIGMA. That is, the seed of OID assures the perfect forwards secrecy of One-Tisme-ID, solving the duplication problem of OID. It also provides a simple key exchange protocol that requires only two rounds, while P-SIGMA requires three rounds. It also extends the application of using the OID method to encrypted communication. [13]

However, this method still has some problems. Since it uses the Diffie-Hellman key exchange mechanism for generating the private information of the next session, it utilizes computing resources a lot. Responders are charged with some computing overhead in calculating OID. This method also cannot generate a dynamic seed for dual-authenticated key exchange that could be changed according to the given security level and the client environment. That is, it uses a fixed initial seed.

2.2 P-SIGMA

The P-SIGMA solves the problems of personal privacy exposure and DOS attacks by using One-Time-ID or simply OID. The OID is an identity that can be used only once for identifying a user. In P-SIGMA, all OID values are unique by means of sequence numbers and one-way hash functions with collision resistance. Thus, an adversary who does not know a secret key cannot predict the OID that will be used in the future, while both users can calculate any OID values.

However, an adversary can guess all OIDs that have been used previously and will be used in the future if he can obtain a secret key, say K, because a fixed secret key is used for calculating all OID values. It implies the impossibility of perfect forward secrecy for OID. Moreover, an adversary who obtains K can impersonate a user in any future session. If a user shares the same OID with multiple communication partners, he cannot decide whom the connection is from, even when he checks the One-Time-ID. [14]

2.2 Active Network

ANTS(active network Transfer System) as the early-stage research creates the structure of active network and the composite research results that makes data packet include programming code and installs the necessary functions to the active node. Also, SwitchWare that strengthen the flexible programming for the safety of network structure and security is suggested, too. ABone(active network Backbone) which figures out the difficulty of preparing the realistic structure of active network designs packet structure and support a variety running environment. These existing researches become a basis for the further studies of active network.

This paper classifies two transmission methods for the composition of the safer active network. The first one is the discrete approach that firstly divides program code and data, and transmits them. The second one is the capsule method that integrates program code and data as the active packet and transmits them. The capsule method creates “active packet (capsule)” that contains program code and data without saving program code at active node, and transmits it to the network. Secondly, active node divides the program code and data from the received active packet. The third procedure is loading program code to the runtime environment in active node, and process data by program code. Finally, they recombine program code and processed data and creates active packet and transmits it to the next active node. ANTS project in MIT and PLANet in Pennsylvania are using this method, but when the program code is very large, the capsule method has many problems, such as traffic overhead, if packet is lost then packet re-transmission, so the efficiency can be reduced. The discrete approach divides program code and data before transmission. It means the program code is installed at active node before the execution. The active node user transmits data with program code identifier. Secondly active node which receives packet checks the identifier and run the proper program code at the active node. Thirdly, it uses running program to process data, and finally it creates packet from the processed data and transmits it. ActiveIP and SwitchWare researched active network with this method. The Discrete approach can be adapted to the only already-installed program code, and the only network manager can add program code, so it is impossible to add the new program that the generic active hosts want to add. This paper uses the Discrete Approach, and resolves its weak point.

3. Wireless Communication

3.1 Scenario

3.1.1 The Security of Active Network : The active network should provide the solution for authentication, authorization and integrity to support the basic security service. In the Discrete Approach, the authentication of program code sender and the secret and integrity of the program code itself are the essential security points. If the program code is modified on bad purpose or it has the potential problem, it will become the unexpected error, so not only low performance of the entire active nodes but also a big security problem will be raised. In addition, if the authentication of program code is not performed, the hacker will modify the program code, and it will be a serious security problem. Now many projects of active network security, such as SANE, Seraphim, PLAN and Safety-Net are ongoing, but they cannot assure the basis of safety in the active network. Therefore, new security system that removes weak points is strongly necessary

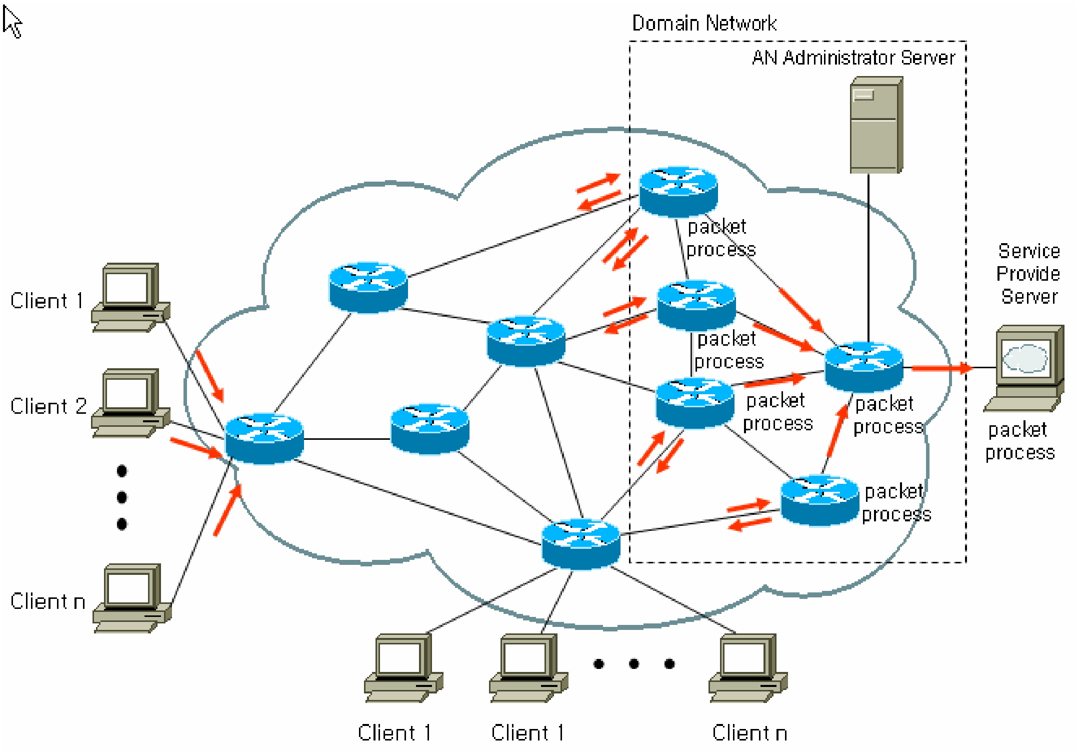

Figure 2 Active network topology [16]

A review was done in an existing study, the security model that provides the basic security solutions such as authentication, authority, integrity is necessary. If the basic security problem is ignored, the performance of the entire active network node will be lowered, and the privacy violation and network congestion will be caused.

To resolve these security threats, we should authenticate active node users on the screte Approach. To authenticate active node users, we can restrict the access of hacker who tends to transmit the offensive program code, and block the forgery of program code. Also, we can reduce the deterioration of performance that the program reinstallation in active node causes through the management of frequently using program code. The active network structure that we propose is shown at Figure 2.

This study utilizes this scenario and use the discrete approach for the authentication proposed below. The active node management server authenticates and manages program codes, too. The active node server authenticates clients and the clients register the program code at the active node management server. The proposed system focuses on the authentication of middle node and the safe transmission of program code in active node. In

3.2 Attacks in Wireless Communication

Many reasons are presented why wireless internet network are at risk, from a security point of view. Wireless Internet networks, do not have centralized machinery such as a name server, which if present as a single node can be a single point of failure. Wireless links between nodes are highly susceptible to link attacks, which includes the following listed below [4]

- Physical Attack: It gets rid of temper-defense-package in chip and then explains main information to put on prove on IC (Integrated Circuit) chip. We analyze electron-wave which emits from attacking prove, communication devices and computer.
- Denial of Service: It is a mean of attack which emits obstructive wave having special frequency for normally not to operate.
- Message loss: It can lose a part of communication method which reciprocates between tag and leader, cause by intention of attacker or error of system. Spoofing: It is a method which passes the authentication-process that individual which is unfair, deceives like to fair.
- Location Tracking: Attacker (invader) or leader, who is sinister, perceives position of tag. So it is a type which disturbs user's privacy by method which grips moving path of tag- owner.
- Traffic Analysis: Attacker (invader) analyse contents which get from eavesdropping and then can predicts tag's answer which is about leader's inquiry.
- Eavesdropping: Attacker (invader) can hear without big effort because communication method which is between tag and leader, is wireless.

Attacks typically involve only eavesdropping of data whereas active attacks involve actions performed by adversaries, for instance the replication, modification and deletion of exchanged data. External attacks are typically active attacks that are targeted to prevent services from working properly or shut them down completely. Intrusion prevention measures like encryption and authentication can only prevent external nodes from disrupting traffic, but can do little when compromised nodes internal to the network begin to disrupt traffic. Internal attacks are typically more severe attacks, since malicious insider nodes already belong to the network as an authorized party and are thus protected with the security mechanisms the network and its services offer. Thus, such compromised nodes, which may even operate in a group, may use the standard security means to actually protect their attacks [6, 7, 8].

As a summary a malicious node can disrupt the routing mechanism employed by several routing protocol in the following ways: [9]

Attack the Route Discovery Process by:

- Changing the contents of a discovered route.
- Modifying a route reply message, causing the packet to be dropped as an invalid packet.
- Invalidating the route cache in other nodes by advertising incorrect paths.
- Refusing to participate in the route discovery process.

Attack the Routing Mechanism By:

- Modifying the contents of a data packet or the route via which that data packet is supposed to travel.
- Behaving normally during the route discovery process but drop data packets causing a loss in throughput.

Launch DoS Attacks By:

- Sending a large number of route requests. Due to the mobility aspect of MANET's, other nodes cannot make out whether the large numbers of route requests are a consequence of a DoS attack or due to a large number of broken links because of high mobility.
- Spoofing its IP and sending route requests with a fake ID to the same destination, causing a DoS at that destination.

The above discussion makes it clear that wireless networks are inherently insecure, more so than their wire-line counterparts, and need vulnerability diagnosis schemes before it is too late to counter an attack. If there are attacks on a system, one would like to detect them as soon as possible (ideally in real time) and take appropriate action. In this kind of communication authentication is necessary a method with different knot of confidence level which would satisfy privacy of user's position.

3.3 Malignant code and Worm

Among the various types of system threatening codes such as virus, Worm and Trojan virus, internet worm is the most dominating system damaging factor. In DOS age, Worm was treated as non harmful code even though it copy and reproduced by itself continuously, it never contaminate the existing other files and system. As the development of network and internet, Worm also evolved to produce damages to system but its original l characteristics are never changed at all. The original worm of DOS ages is call as just Worm but current worm is called as I-Worm (Internet Worm).

Worm of prototype just create so many useless trash files by copy itself continuously and it is not so harmful to system but I-Worm decrease the system speed seriously by attempting copy through the network. During past few years, many different types of I-Worm were created. As a result of it, I-Worms are classified by two different types such as Network Worm and Internet Worm according to its propagation ways. If it is propagated through local network, it is called as Network Worm and if it is propagated through global network like internet, it is called as Internet Worm. Internet Worm is classified into three categories according to PC infection method. First group of Internet Worm is activated by just reading e-mails. Second group is activated by opening attached files of e-mail. Third group is activated by itself without any PC user's action. Also E-mail Worm is classified as Slow mass-mailers and Fast mass-mailers depending on its dissemination speed. Slow mass-mailers Worm is transferred at the same time when the infected PC users send an e-mail and Fast massmailers Worm is disseminated to many e-mail users at once. E-mail Worm use the email client such as Microsoft Outlook and Outlook Express to disseminate the worm to other PC users and it is transferred at the same time to all the users whose e-mail addresses are listed in specific mail client. On that way, if one is infected by e-mail worm then so many other PC users whose e-mail addresses are stored in an infected PC have possibilities of infection. This chain reaction can cause great amount of PC infections and damages in very short time. Current trends of e-mail worm such as Loveletter and Navidad, use very sensitive words which stimulate the PC user or use the title that lewd photos or video files are attached. Moreover, recent e-mail worm disguise that updated virus vaccine files are attached. These methods evoke the PC user's curiosities to open attached files or e-mail without any doubt. Network Worm is disseminated by local network system and is consist of next three steps.

- Find a Shared Drive
- Mapping Drive
- Copying Worm and Execute

In general, copied worm is not activated immediately and it is stored at starting folder which can be executed automatically with the start of Window. So the copied worm can be activated automatically at the reboot of system. Netlog is one of the Network Worm. Netlog set the IP to search the dissemination target and find out the system which is share the entire C drive in whole subnet system. Then, set the target drive by J drive and copy the worm to Window folder and Window Start folder to make it activated for infection at next start of Windows.

Window Worm is one of the dominating Internet Worm nowadays and there are two types of Window Worm depending on which type of platform they use. Window Worm is activating at Window system and Non-Window Worm is activating at different platform. Window Worm makes use of e-mail, newsletter, IRC, MSN Messenger, Gnutella, IIS and other chatting programs. Most well know Non-Window Worm of love-letter concept is Morris Worm which is activating at Macintosh and UNIX system such as Linux and Solaris. Linux Ramen Worm is first Non-Window Worm which produced tremendous amount of damages. Also the As mind of Solaris and Simpson of Macintosh is other types of Non-Window Worm which can be found recently.

4. Preceding Authentication Method

There is an existing hash based authentication method Figure 3 which is proposed by Henrico and Muller[10]. This method is a protocol which prevents location tracking by updating ID based on hash. Manufacturer constructs database which can save h(ID), ID, TID, LST, AE and save ID, TID and LST in TAG. The TAG which received query increases 1 of TID and calculates h(ID), T=h(TID xor ID), TID and transmits to

READER. The database searches ID with h(ID) and calculates T' which is added pertinent TID to ΛTID. In [Fig 1], If T and T' are same in Behaving of (3), Database calculates and transmits Q and xor calculates randomly generated R for updating ID. The tag which received (5) also calculates Q' and compares with Q. If both Q' and Q are same, the tag updates its ID. AE is designed safe from errors in system or losing messages by attacker. Because AE has previous ID information.

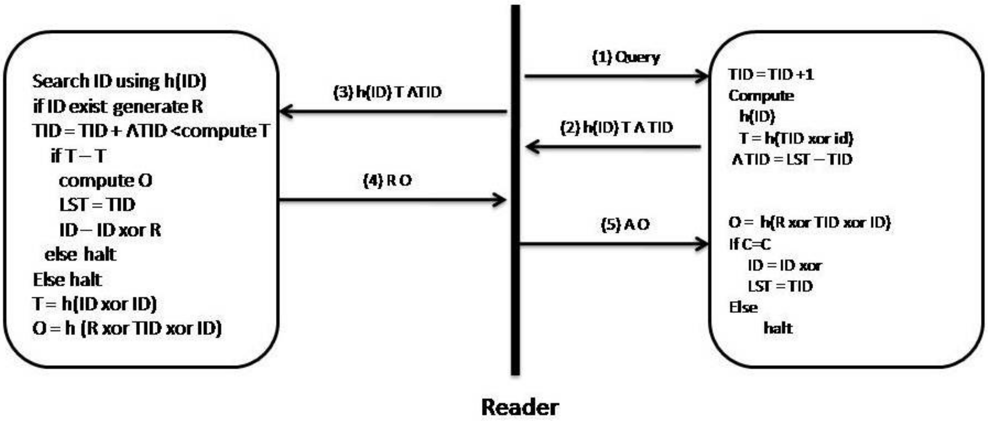

Figure 3. Authentication Protocol based on hash [11]

In the perspective of the location tracking this method is safe because the ID updates when authentication process is over. In case of abnormal authentication processing between TAG and database that is attacker send query to TAG for attack, The attacker can do location tracking attack to TAG because The TAG always replies corresponding h(ID). If the TAG transmit (2) in session with database before opening normal authentication session, database is authenticated to attacker as normal TAG. Attacker give R that continuous character string which consists of 0 in the value of (5) that READER transmits to TAG in the middle of session. And then, attacker transmits T instead of Q. Therefore, the TAG can't notice error. When next authentication processing, server can find existed ID with h(ID). However, there is an disadvantage that TAG can't receive authentication, existing ID about LST is not corresponded with saved TAG and database. There is another method that READER generates random value S with Pseudo random number generator and query to TAG previously [5]. However, these methods have an disadvantage. If the 3rd person send spoofing query to TAG as READER, the TAG can't notice normal user or not. Of course, several advanced methods are proposed to solve the disadvantage. But they can't solve original problem.

5. Suggested Authentication Method

As suggested in [11] a new authentication method which is safe against spoofing attack and reducing hash time that 2 of hash function time reduce one in tag calculation time. This is shown in Figure 4. This method is similar to ID transformation protocol based on advance hash [12]

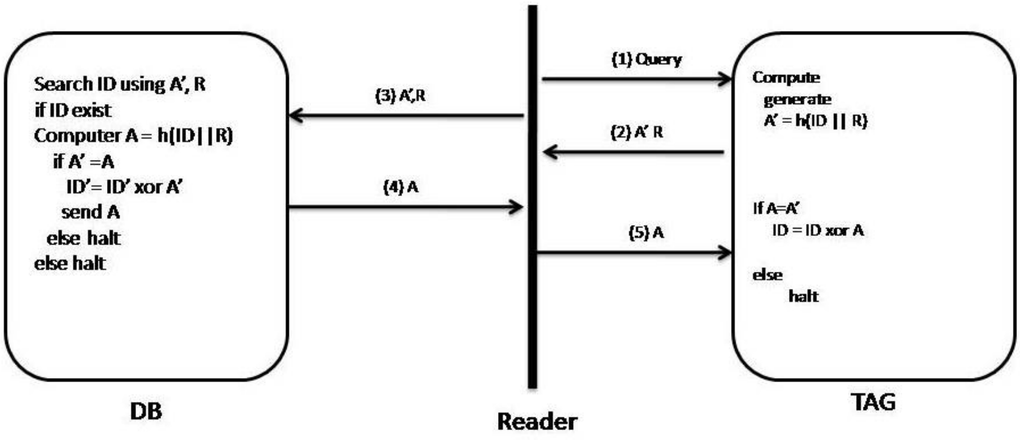

Figure 4. Suggested Authentication Method [12]

This is done as of the following, first TAG makes random value R from pseudo random number generator and then, creation A'=h(ID||R) and then, A' and R transmit to DB through READER. DB is searching ID through A' and R and creating A=h(ID||R). DB compares A with A'. If both are same, DB authenticates the right TAG and updating XOR calculating ID to A' then transmit it to TAG. TAG compares A with A' and if both are the same, TAG calculates ID=ID xor A.

The authentication process is summarize in the following:

```
query to TAG                             /*Reader*/
generate R;                        /*Tag*/
compute A' = h(ID||R);
send (A',R) to READER
bypass to DB;                            /*Reader*/
search ID using (A',R)                   /*DB*/
if ID exist
     computer A=h(ID||R);
     if A'=A
             ID'=ID' XOR A';
             Send A to READER
bypass to TAG;                     /*Reader*/
if A=A' then ID=ID=XOR A;                /*Tag*/
```

6. Proposed Key Exchange in Authentication Mechanism

The key exchange mechanism proposal in [15] has three phases. The first is a preliminary setup phase. In this phase, public information and random number matrix of an initiator are delivered to its responder. In the second phase, the initial seed is generated which is used to create a shared secret key for the data communication session. The third phase performs dual authentication between communication parties and creates a data encryption key that are shared.

6.1 Model and Notation

An entity which initiates a key exchange mechanism is called an initiator, and an entity which responds to the initiator's request is called a responder. Both are kinds of user. Another type of entity which is not a user but an attacker is called an adversary. An adversary is a Polynomial-Time Machine that attacks the secrecy of key exchange mechanism. The following table summarizes the notation used in the proposed mechanism of [15].

Table 1. Notation

$g_1\ (k)$	A generator created by the initiator at the k-th time
$h\ ()$	A cryptographic hash function
$MX[m,n]$	A random number at the [m,n] cell of the random number matrix MX[,]
$Y_1(1),\ Y_1(2)Y$	Initiator's first and second public information
$X_1(1),\ X_1(2)$	Initiator's first and second secret information generated at random
$E_X\ (Y)$	Encryption Y using X
$OID_1\ (k)$	One-Time-ID generated by Initiator at the k-th step
C_1	Challenge generated by initiator
$R_1{}^C{}_R$	Response to the responder's challenge, generated by initiator
CM_1	Encrypted challenge message generated by Initiator
$AK_1{}^C{}_1$	First authentication key generated by initiator for initiator's challenge
$\mathrm{WK_S}$	Data encryption key (working key) in the s -th session
$\mathrm{AK'_1{}^C{}_R}$	Second authentication key generated by initiator for responder's Challenge
$EWK_1\ (s)$	Encrypted working key generate by initiator in the s -th session

6.2 One-Time-ID(OID)

The OID is an identity that can be used only once for identifying a user. One-time-ID can be used to protect DOS attacks and man-in-the-middle attacks. To prevent DOS and man-in-the-middle attacks, OIDI(i) is attached at every i-th message transmission

OIDI(i) = h([m,n], MX[m,n], j)

OIDI(i) is a hash function of [m,n], MX[m,n], and j, where [m,n] is a random position among the random numbers assigned to the initiator within the random number matrix, MX[M,N], and j is just a random number in i-th message transaction. By using [m,n], we can detect DOS attacks and also decide who the initiator is. Man-in-themiddle attacks are detected by checking whether the transferred hash value is correct or not. For message integrity, we attach the hash value of all of the parameters transferred together at each message transmission.

6.3 Phases

In the preliminary set up phase, preliminary number are generated and delivered to the opposite side for the next phase. For the Diffie-Hellman key exchange, the initiator side generates $X_I(1)$, g_I (1),p $_I$ (1) and deliverits public values to the responder. Fro the purpose of protecting it from DOS attack and Man-in-the-middle attacks using One-time-ID, the responder generates a MxN random number matrix and assigns them to the initiator. Be careful, however, that the same cell should not be assigned to different initiator. The responder should save the cell assignment information. This information is used for protecting against DOS attacks.

The initial seed generation phase is used to create a shared secret key for the first session. In this phase, the initiator sends a challenge message to the responder in order to authenticate the responder according to the Hughes method. In contrast, in the second step the responder sends a challenge message to the initiator for authentication according to the Diffie-Hellman method. In t eh third step, the initiator and the responder are authenticated according to the corresponding methods, respectively.

The authentication and key exchange phase is in the sth session. Each party has the same seed that can be used to create the shared secret key. At the first step the initiator sends OID $_I$(1) that includes AK $_I$(S) as a member of hash input. Using this value OID $_I$(1), the responder can know whether the sender has the correct shared secret key or not, authenticating the initiator. The working key WK_S is used as the shared data encryption key during the sth session.

7. Analysis

A safe authentication method presented in Section 5 and particularly by using the proposed key-exchange mechanism generates a scheme that provides exceeding security to an unsecure communication. The key exchange method [15] was proven to provide dual-authentication key exchange mechanism as well as data integrity and data confidentiality. The existing method IKE and P-SIGMA are based on the fixed seed of shared key like One-Time –ID and an authentication key. Accordingly, if the culprit knows the fixed secret information, one can impersonate the initiator in the future session.. in contrast, the proposed scheme can regenerate the initial seed dynamically depending on the current client environment or adapting to the change in the security level. Because the proposed system does not use public key cryptography like Deffie-Hellman and RSA, which requires much computing power, it can be used for thin clients like mobile or ubiquitous computing devices. Moreover, the proposed system is so efficient as to finish within two messages round for authenticated key exchange.

Aside from that, the scheme provides more concrete protection against DOS attack and Man-in-the middle attacks.

8. Conclusion

This paper proposed an efficient dual authentication key exchanged in an active network scenario. The proposed system does not require the public key cryptography like Diffie-Hellman and RSA and certificates. The scheme protects personal privacy of identity information. It also provides an effective method to protect against DOS attacks with the scope information of initiator's random number table sent by the responder.

References

[1] Gross, Ralph; Acquisti, Alessandro; Heinz, J. H. (2005), "Information revelation and privacy in online social networks", Workshop On Privacy In The Electronic Society; Proceedings of the 2005 ACM workshop on Privacy in the electronic society, pp. 71-80, doi:10.1145/1102199.1102214

[2] 3. R. Koodli and C. Perkins, "Fast Handover and context Relocation in Mobile Networks, "ACM SIGCOMM Comp. Commun. Rev., vol. 31, Oct. 2001.

[3] M. Balazinska and P. Castro, "Characterizing Mobility and network usage in a Corporate Wireless Local Area Network, "Int'l. Conf. Mobile Systems, Apps, and Services, May 2003.

[4] Sungho Yoo, Kihyun Kim, Yongho Hwang and Piljoong Lee, H. "Satus-Based RFID Authentication Protocol," Journal of The Korean Institute of Information Security and Cryptology, Volume 14, Number 6, pp. 57-67, December 2004.

[5] Wikipedia.org

[6]. S. Pack and Y. Choi, "Pre-Authenticated Fast Handoff in a public Wireless LAN based on IEEE 802. 1x Model," IFIP TC6 Pers. Wireless Commun., Oct. 2002.

[7]. M. Nakhjiri, C. Perkins, and R. Koodli, "Context Transfer Protocol," Internet Draft: draftietfseamoby-ctp01.txt, Mar. 2003.

[8]. R. Perlman, "An Algorithm for Distributed Computation of a Spanning Tree in an Extended LAN," 1985, pp. 44-53.

[9] Byoung-Muk Min, Sok-Pal Cho, Hong-jin Kim, and Dong Chun Lee,"System Development of Security Vulnerability Diagnosis in Wireless Internet Networks", Computational Science and Its Applications-ICCSA 2005.

[10] Dirk Henrici and Paul Muller, "Hash based enhancement of location privacy for radio frequency identification devices using varying identifiers," PerSec'04, pp. 149-153, March 2004.

[11] Hoon Ko, Bangyong Sohn, Hayoung Park, and Yongtae Shin "Safe Authentication Method for Security Communication in Ubiquitous" Computational Science and Its Applications-ICCSA 2005

[12] Youngjoo Hwang, Misoo Lee, Donghoon Lee and Jongin Lim, "Low-Cost RFID Authentication Protocol on Ubiquatous." CISC'S04, pp. 120-122, June 2004.

[13] H. Krawczyk, The IKE-SIGMA Protocol, Internet Draft, 2001

[14] Kenji IMAMOTO, Kouichi SAKURAI, A Design of Diffie-Hellman Based Key Exchange Using One-Time ID in Pre-shared Key Model, AINA'04. IEEE, 2004.

[15] Yonghwan Lee, Eunmi Choi , and Dugki Min "An Authenticated Key Exchange Mechanism Using One-Time Shared Key", Computational Science and Its Applications-ICCSA 2005.

[16] Jin-Mook Kim, In-sung Han, and Hwang-bin Ryou "An Active Node Management System for Secure Active Networks "Computational Science and Its Applications-ICCSA 2005