International Journal of Security and Its Applications
Vol. 10, No. 10 (2016) pp.135-146
http://dx.doi.org/10.14257/ijsia.2016.10.10.13

Experimental Analysis using Robust Key Exchange Authentication Scheme in Mobile Ad-hoc Environments

Cheol-seung Lee

Dept. of Teacher Training & Liberal Arts, Kwangju Women's University
Gwangju, Korea
cyberec@kwu.ac.kr

Abstract

A network of autonomous by multiple mobile nodes with a wireless interface in the absence of a particular network infrastructure environment is referred to as Mobile Ad-hoc network. The demanding in construction of the stand-alone networks and interconnection between convergence devices have led an increase in research on Mobile Ad-hoc Network and the application of Mobile Ad-hoc environments has been paid much attention as a wireless computing which is growing fast in the field of computer engineering With performance both as hosts and routers, easy network configuration, and fast response, mobile nodes participating in Mobile Ad-hoc Networks are suitable for mobile computing but have vulnerable points, about lack of dynamic network topology due to mobility, network scalability, passive attacks and active attacks which make it impossible to manage continuous security authentication service.

In this study, proposes Session key-Encrypted key exchange authentication mechanism for a robust authentication based on Mobile Ad-hoc Network and through identify wireless environment security vulnerabilities, currently being used in OTP S/Key and DH-EKE analyzes.

Keywords: *Mobile Ad-hoc Network, DH-EKE, EKE*

1. Introduction

Although Mobile Ad-hoc Network is suitable for Wireless computing application because mobile nodes conduct host and function of router, unstable link, data transmission error, network expandability and the denial of service *etc*. those have a lot of weakness in security on passive and active attack [1-2].

In order to solve vulnerability in security of security authentication caused by Mobile Ad-hoc Network in this dissertation, it analyzes a routing protocol and authentication technic, suggests Session key-encrypted key exchange authentication technic which provides security five-factor and has strong belief.

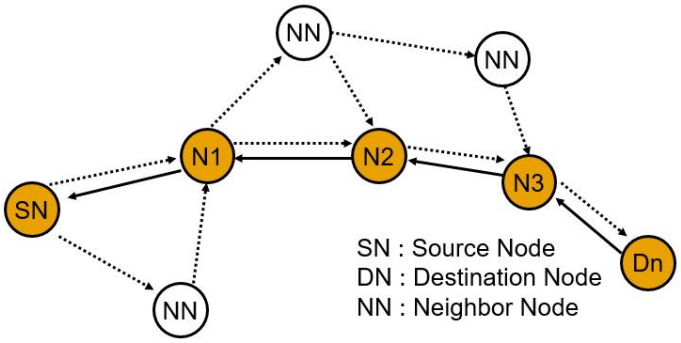

Figure 1. Mobile Ad-hoc Network

ISSN: 1738-9976 IJSIA

2. Mobile Ad-hoc Network Security Environment & Authentication

2.1. Mobile Ad-hoc Network Security Environment

A Mobile Ad-hoc Network routing protocol could response rambling mobile node immediately each time a connection request, research of On-demand system which could reduce overhead by control traffic forms main trend [3-4].

AODV(Ad hoc On demand Distance Vector) based on DSDV(Destination Sequenced Distance Vector) which has a system of On-demand supports all unicast and multicast, prevents routing roof using sequence number of destination node and can improve entire network performance due to reducing unnecessary transmission frequency [5].

However, it has been exposed to a variety of threat and attack owing to playing a transmitted role through multi hop between the mobile nodes, Also, there is a security vulnerability between the mobile node due to malicious node and compromised mobile node are camouflaged as work normally [6-8].

2.2. Mobile Ad-hoc Network Threat and Attack Pattern

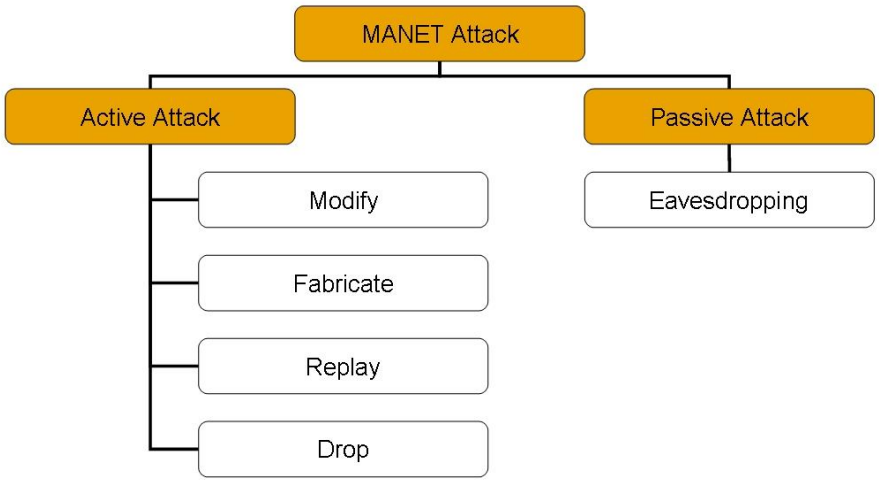

Figure 2. Mobile Ad-hoc Network Attack Pattern

The Mobile Ad-hoc Network is short of physical defense about malicious nodes from unsafety links, limited frequency, transmission distance, energy limitation between mobile nodes and interference of electric wave resulted from increase in the mobile node. Also, it could be exposed to a variety of threat and attack pattern due to data integrity, problem of the confidentiality, limitation of security mechanism, absence of CA (Certificate Authority).

Outside threat of the Mobile Ad-hoc Network is classified into inserts of incorrect routing information, regeneration and transforming. Malicious nodes divide networks or lead to errors of entire networks with causing of heavy traffic through the outside threat.

Internal threat is caused in the damaged mobile node provides incorrect information for the mobile nodes and occurs the networks' errors. The method which would cope with both outside threat and internal threat efficiently should make a detour around the damaged mobile node with the sufficient mobile nodes. The Mobile Ad-hoc Network has active and passive attack patterns because it makes the mobile node transmit data through multi hop. Also, the mobile nodes compromised malicious nodes look like working normally but, they might distort the networks of routing structure so it exists security weakness between the mobile nodes and needs reliable Mobile Ad-hoc Network security technics [9].

2.3. OTP S/Key Authentication Protocol

Authentication protocol of Mobile Ad-hoc Networks are divided into PKI (Public Key Infrastructure) base and authentication technic using OTP (One Time Password) according to the fact of existence or nonexistence.

OTP S/Key (One Time Password Session Key) using session key has a simple arithmetic operation process and might ensure mobility in consideration of weak point and performance degradation might be caused by authentication. OTP always creates different hash code and authenticate the mobile node according to conforming or nonconforming regarding preserved value of destination node following addition calculation. OTP S/Key depends on source node of secret key completely, all confidential information is H() is encrypted and stored. Also, compare to Time synchronization, challenge-response and authentication technic, stability, practicality and simplicity is outstanding but authentication technic using OTP still has a lot of problems.

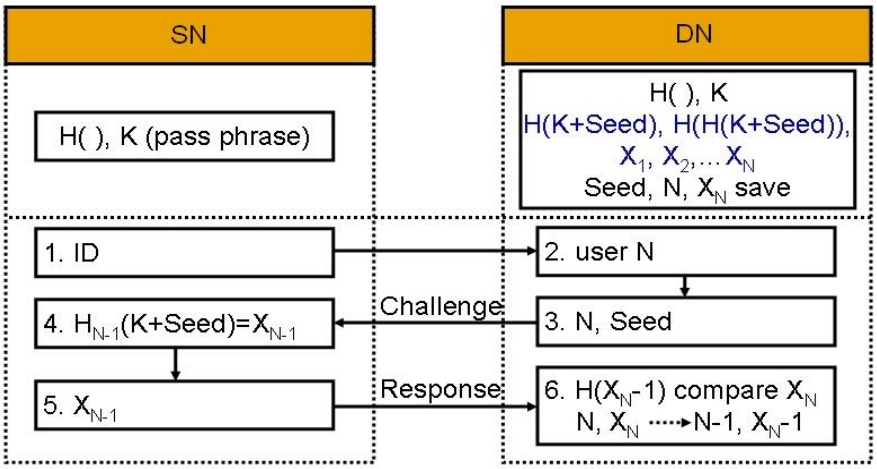

Figure 3. OTP S/Key Authentication Protocol

2.4. DH-EKE Protocol

DH(Diffie-Hellman)-EKE(Encrypted Key Exchange) is made up of object authentication, key freshness, key confirmation and key agreement in the manner of exchanging session key and is a protocol which generates session key after generating each of the random numbers from network participants in order to improve Denning-sacco attack vulnerability of EKE Protocol. As the Figure 4 DH-EKE Protocol, network participant A chooses own random number A^R ,exponentiation A^R of Primitive roots g of big decimal P and transmits to B following encryption with A^{ID} using shared password $H(P)$ with B. B descrambles received messages to $H(P)$ and works out the answer after that generates session key K with exponentiation B^R of own random number. B codes own public key g^{BR} to $H(P)$ transmits to A with coding check value $Challenge_B$ to K.

A let received message decoded and generates g^{BR}, after that private key A^R of A Passed away at the index, makes $K=g^{BRAR}$ and let $Challenge_B$ decoded using K. A transmits to B by encrypting the check value $Challenge_A$ and their $Challenge_B$ to K to confirm key. B let received encrypted message decrypt K and check that share the same session key in accordance with whether or not the match $Challenge_B$ received from the A and B and authenticate $Challenge_A$. And $Challenge_A$ encrypts K transmits to A, A authenticates B after checking whether or not match of the received $Challenge_A$.

However DH-EKE is safe from a password guessing attacks , Denning-sacco to use public key and *K*, vulnerable to a password premeditated attacks, Stolen-verifier attack, when applied to the MANET, it requires credible session key exchange authentication techniques provided routing security and mutual authentication [10].

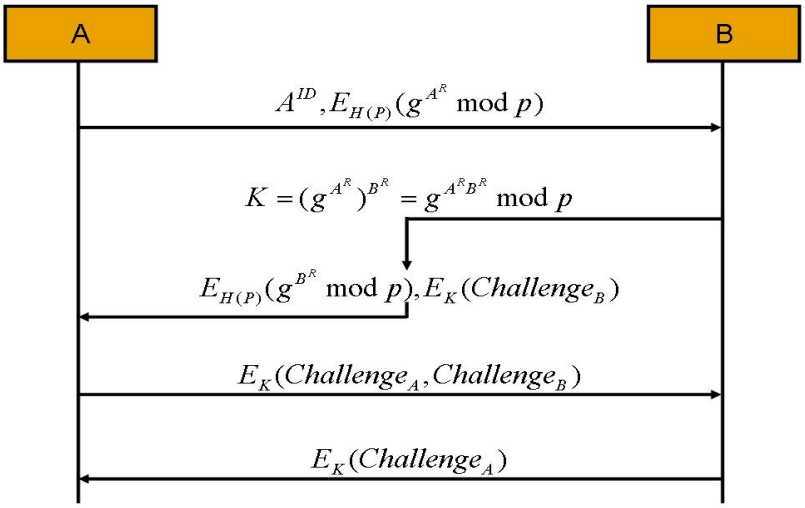

Figure 4. DH-EKE Protocol

3. Session Key Exchange Authentication Scheme

This paper is the credible session key exchange authentication techniques which are for Mobile Ad-hoc Network routing security certification, a hash routing and OTP S/Key applies to DH-EKE so that they can cope with dynamic network topology immediately.

Session key-EKE was configured as an authentication system using an encrypted password validation, and the key exchange step and the step for routing mobile node authentication for secure communication path secured. The mobile node can generate a hash table for being routed around the OTP generation and may derive multiple sets of public key element from the hash table. Each mobile node may be a password verifier $H^n(p)$ to ensure the integrity of the encrypted message routing secure route determination through H(AODV) combines OTP in AODV(Ad-hoc On-demand Distance Vector) [11].

The verification step of the authentication and key exchange of the mobile node registering the hashed passed password verifier $H^n(p)$ by applying the MD(Message Digest)5 and the session was a common way to exchange a session key between the mobile node after the connection.

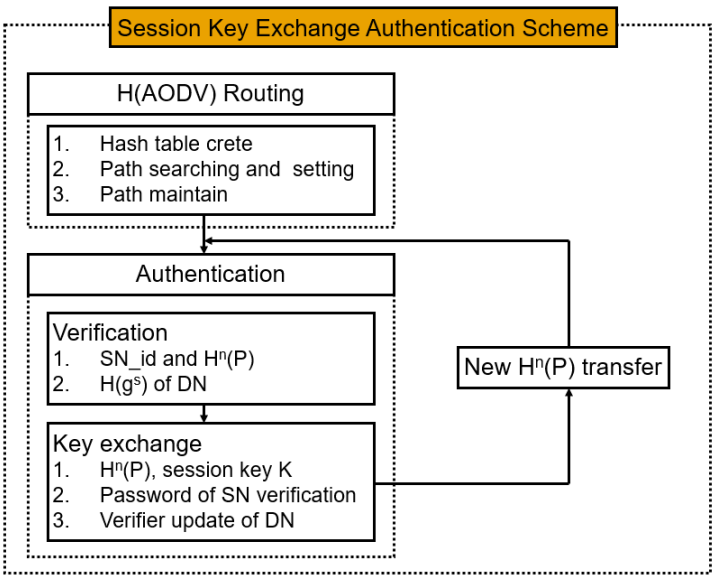

Figure 5. Session Key Exchange Authentication Scheme

3.1. Routing for Ensuring Secure Communication Path

Source node to ensure a secure communication path transmits the route search message to the destination node with the neighboring nodes.

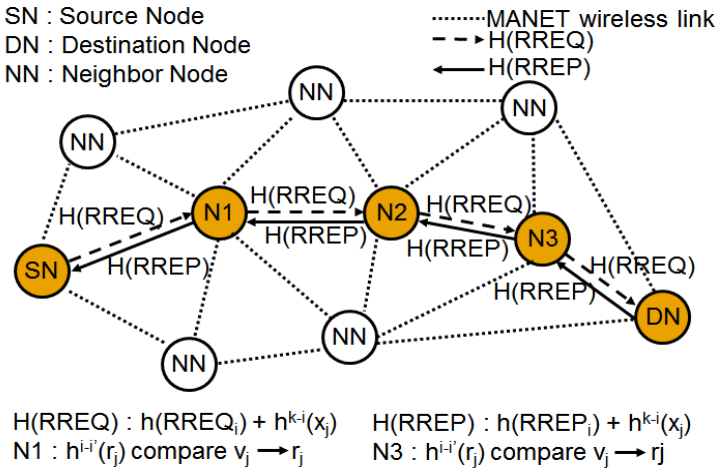

Figure 6. H (AODV) Routing Protocol

As it is shown in Figure 6 source node 448 mod 512 by applying a signature to the i-th route search message to be transmitted, and generates the integrity-guarantee $H(RREQ_i)$. log_2^n bit is added to the message in order to form a single private key x and a public key to generate a signed message, an additional bit of y to each bit of the signature of the message source node. Calculating the number of bits of 0 in $H(RREQ_i)$ to be added to the $H(RREQ_i)$ and have the bit string g of n bits. Find the j-th bit string g_j is 1, the $h^{k-i}(x_j)$ the hash value in the *(k-i)* the row of the hash table generated for each mobile node for all j in addition to the H(RREQ) it is transmitted to the mobile node.

H(RREQ) neighbor node has received the message is for digital signature verification by applying MD5 to get $H(RREQ_i)$ calculating the log_2^n and by calculating the number of bits in the message and added to the column, 0 $H(RREQ_i)$, and *n* bit generates a string

value g. It is checked whether the j-th bit string of $h^{i-i'}(r_j)=v_{j,}\, gj = 1$ for all j. r_j is the OTP of the currently transmitted H(RREQ), v_j is the H($RREQ_{i'}$) OTP. When $h^{i-i'}(r_j)=v_j$ is a guarantee that the same can be seen that the integrity of the routing information, the integrity of the routing information, the mobile node verifies the H(RREQ) to update the v_j for verification and then H(RREQ) to the search value r_j repeat the forwarding process from the source node to destination node performs. Destination node receiving the H(RREQ) from the source node is transmitted via the reverse path to generate a response message H(RREP). Neighbor node receives the i-th H($RREP_i$) of the destination node from a destination node can secure routing path by repeatedly performing the following H(RREP) search and update the value v_j by r_j for forwarding to verify from neighbor node to the source node procedure [9].

3.2. Verification and Key Exchange for Authentication

3.2.1. The Source Node Registration and Verification: In the registration phase, and source node is transmitted to the destination node with the n-th *SN_id* password verifier $H^n(P)$, destination node is saved and then the received *SN_id*, $H^n(P)$ in the password directory, source node is transmitted to the public password $H(g^s)$ for authentication between source node and destination node. Source node has only to remember their passwords, Password of the source node can be prevented from being exposed directly because destination node is stored only $H^n(P)$ of the source node.

After the registration process, the validation phase of the source node and destination node based on $H^n(P)$ source node prove the password and It updates the $H^n(P)$ stored in the password directory of the destination node as a validation of the next session. $H^n(P)$ after setting the password, in the $i(i\leq i<n)$ session, the $H^{n-i+1}(P)$ of source node and $H^{n-i}(P)$ of destination node is used as a password verification.

In the first session source node share with destination node through the register that $H^n(P)$, in order to prove ownership of the source node and sends the password to encrypt the $H^{n-1}(P)$. Destination node is hashed once again in the $H^{n-1}(P)$ received from the source node $H(H^{n-1}(P))$ and a value after confirming match whether the $H^n(P)$ stored in the password directory on the destination node, you can see the password values of the source node. The destination node and stores $H^{n-1}(P)$ in the directory and verified in the same way till $(n-1)$th communication, it performs an authentication key exchange phase through generated verification between source node and destination node

3.2.2. Authentication Key Exchange Phase: After performing the initialization of the authentication key exchange phase and the verification phase register stage store $H^n(P)$ of the validation in a hash table and each of the mobile node, produce the session key by performing the encryption between source node and destination node. I-th session process between source node and destination node are shown in Figure 7.

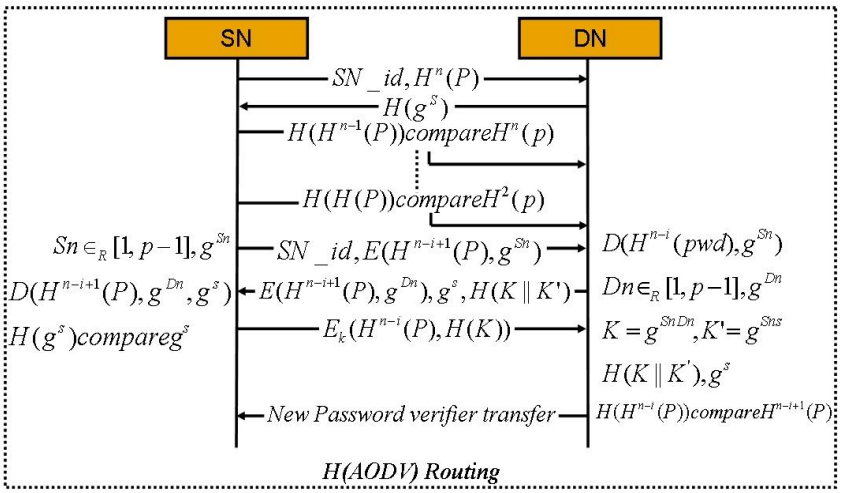

Figure 7. Session Key-EKE Authentication Process

Source node is a randomly generated $Sn \in_R [1, p-1]$ and the key value calculated g^{Sn} for session key generation and, encrypts $H^{n-i+1}(P)$ in which g^{Sn} shared between source node and destination node and sent to destination node with *SN_id*. Destination node is *SN_id*, $E(H^{n-i+1}(P), g^{Sn})$ for receiving and After decoded by the $H^{n-1}(P)$ for the source node is stored in the password directory, extracts g^{Sn}.

Destination node selects randomly generated $Dn \in_R [1, p-1]$ calculate the key value g^{dn} for session key generation, the exponential power of g^{dn} the g^{Sn} using a long-term secret key *s* and the session key *K* after calculation a password verifier *K'* to be used in the following session, The source node and destination node to produce a verification message $H(K \| K')$ to verify whether the value matches the key generated in common.

After verifying key messages generated by the $H^{n-i+1}(P)$ who shared with source node g^s long-term public key and the destination node g^{dn} encrypt and g^{dn}, with $H(K \| K')$ is sent to source node. After receiving the message from the source node is destination node, $E(H^{n-i+1}(P), g^{Dn})$ decodes the character his password verification, by applying a hash function to the long-term public key of the destination node g^s. It maintains a session according to whether the match his public password $H(g^s)$ value.

The key exchange process of the session key-EKE, based on the difficulty of DH-EKE. If you do not know the long-term secret key *s*, although g^{Sn} and g^{Dn} a malicious node would acquire $K' = g^{Sns}$ do not calculated. Therefore, if the destination node is sent to create the key messages properly verified correctly it proves that it knows the long-term secret key *s* of the destination node. After source node is $Sn \in_R [1, p-1]$, g^{Sn} and using the session key $K = g^{SnDn}$ and $K' = g^{Sns}$ calculated, Check the key validation messages $H(K \| K')$ value and verified. And then encrypts the session key $K = g^{SnDn}$ and $H^{n-i}(P)$ to the session message to $H(K)$ is applied to a hash function to *K '*, and transmits a destination node. $K' = g^{Sns}$ is an authentication key used for transmitting destination node the password verifier to the next session of the source node, only source node and destination node is the value that can be generated. Therefore, a malicious node may use the *K'* and send the encrypted password verifier for the source node for the next session because it does not produce a *K'*.

Destination node is decrypted using *K'* from source node check the $H(K)$, check that share the source node and the session key *K* correctly. In addition, by applying the hash function again in the received password verifier $H^{n-i}(P)$, If $H(H^{n-i}(P))$ and the value $H^{n-i+1}(P)$ value of the two values compared to the values that match, destination node is to certify that the source node is to know the password correctly. If the source node and

destination node perform a legal authentication process, destination node is stored in the directory and replace it with a password verifier $H^{n-i}(P)$ of source node [12].

4. Authentication Experimental Scheme and Result Analysis

Experiment of session key-EKE is 0~900/sec was measured while using a Linux-based NS3. CBR (Constant Bit Rate) source node is first started the session by creating a 512byte/sec 4 packets computation of the data packets transmitted to the destination node, using a delay time and the destination selected at random and random waypoint, after it reached its destination at a rate of 0~20m/sec and stays 5 seconds, designed to move to another destination.

MD5 was performed four times the number of settings for password validation generate the initial characters of the proposed scheme, produced large prime number *p*, *g*(*Primitive roots of p*) between source node and destination node. *g* cases when the power of the *p, [1, p-1]* to be a randomly generated, every time a session is changed $Sn \in_R [1, p-1]$ are generated randomly.

4.1. Experimental Environment

Table 1. Experimental Environment

Construction	Experiment
OS	Fedora Linux
Network Simulator	NS3
Language	C, C++
Network	1,000 * 1,000 (m^2), 50 nodes
Simulation Time	0 ~ 900 sec, pause time 5 sec
Mobility	Random waypoint, Random drunken, Trace based
Mobile Node Speed	0 ~ MAX (20m/sec)
Radio Model	Noise Accumulating
Data Link	CSMA, IEEE 802.11, MAC
Network Routing	H(AODV)
Transport	UDP (654 port)
Transport Packet	512 byte * 4/sec
Application	CBR, FTP, HTTP, Telnet

As the Table 1, Experiment of suggestion technic is 0~900/sec was measured while using a NS3 based on Linux operating system.

4.1.1. Design of Mobile Ad-hoc Network Model: The Mobile Ad-hoc Network model for performance evaluation of the proposed scheme was designed. Firstly, according to IEEE 802.11 link layer and the TDMA(Time Division Multiple Access), traffic agents of the mobile node and application services are decided by the CSMA(Carrier Sense Multiple Access) using the mobile node and using the MAC protocol. Secondly, traffic agents determine the UDP which is using in the transport layer. Thirdly, as the work that decides application services transmitting from the application layer protocol, it decides detailed traffic type such as the CBR(Constant Bit Rate), FTP, HTTP and Telnet. Finally, it sets the simulation time 0~900(sec), and measures overhead about the $n/log_2 n$ packet.

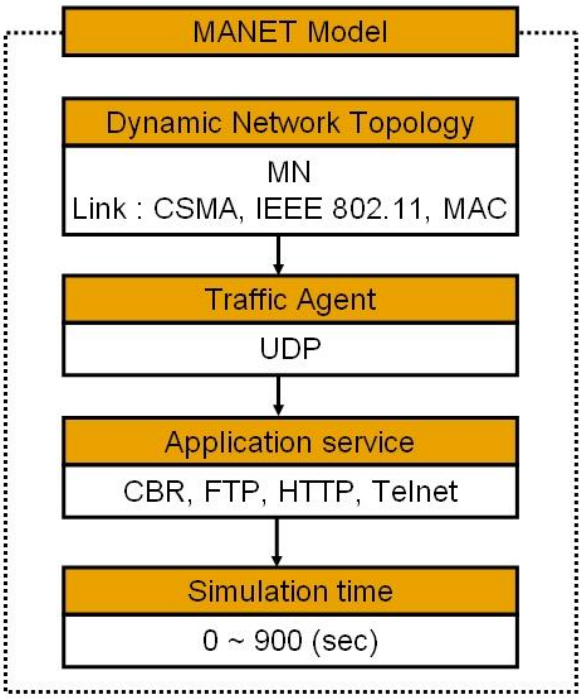

Figure 8. Design of Mobile Ad-hoc Network

4.2. Safety and Efficiency Analysis

Safety routing session key-EKE will provide integrity of the message hop counter field between the mobile node using the H(AODV). In addition, safety for authentication, to generate a new session key through $Sn \in_R [1, p-1]$, $Dn \in_R [1, p-1]$, $H^n(P)$ and secure the replay attack, Moderator attacks can be prevented by using the session key K and mediator attack session key verifier K'.

Since the DH-EKE do not use the source node of the public key of the session key K generated by the source node matrix, Denning-sacco can defend the attack, Offline guessing attacks because the message is encrypted with $H^n(P)$ cannot be estimated with any of the doors or bases plain randomness, it is impossible to know the correct password through a dictionary attack. Even if the password of source is exposed, Safety of the session key is based on the DLP and Diffie-Hellman, it provides a PFS(Perfect Forward Secrecy) secure and provides the security of Stolen-verifier attack.

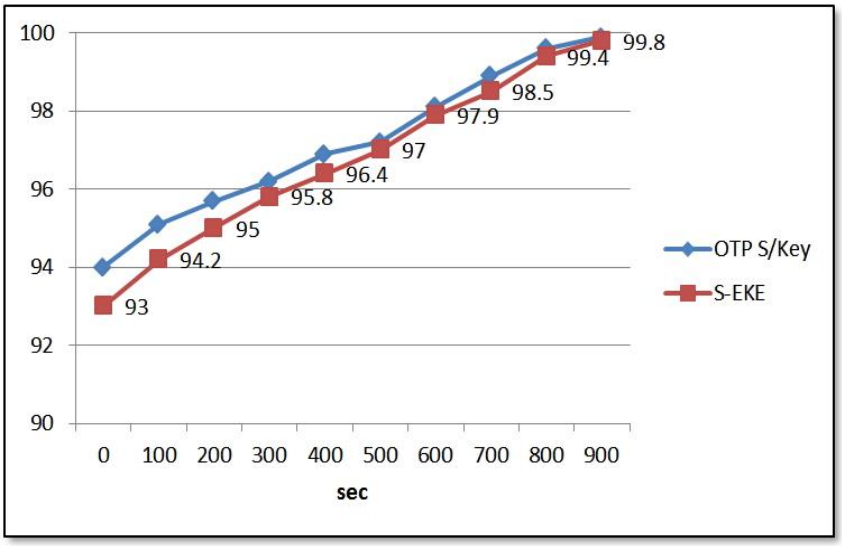

Figure 9. Packet Delivery Rate

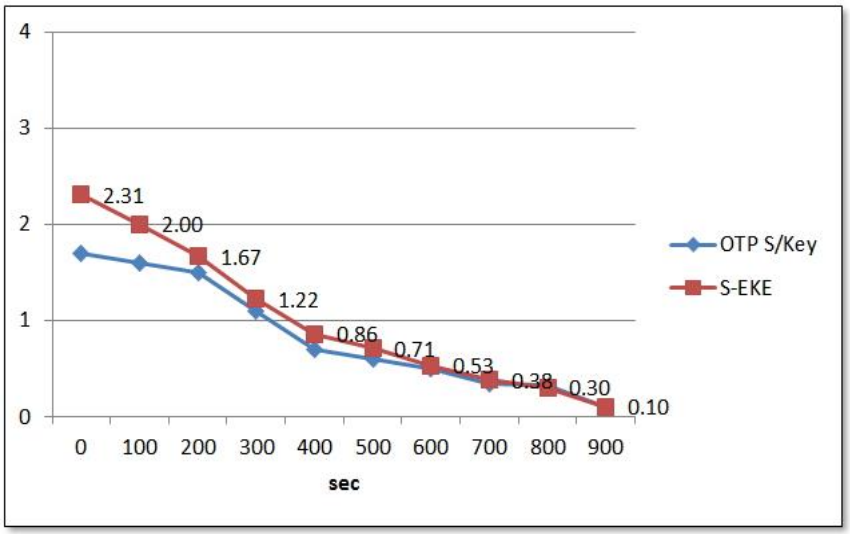

Figure 10. Routing Overhead

Figure 9 is generated by the packet transfer rates cbrgent.tcl, In the case of 0/sec mobile node are moved towards a destination node. OTP S/Key shows a packet transfer rates of 97.16% for the average during 0~900/sec, session key-EKE is showing a packet transfer rates similar to AODV to 96.91%. However, the session key-EKE is the simulation start time 0/sec packet transfer rates are 93.0% for searching for a path falls, after 500/sec, the packet transfer rates can be seen that this increase. 900/sec there proves to be very efficient for searching and setting a path for sending and receiving. The data packet to 99.8%.

Routing overhead refers to the number of control packets, which are required for a CBR session. Figure 10 is connected to 30 nodes of 50 nodes involved in the network, routing overhead measurements. Although session key-EKE have 2.31 of routing packets encrypted with the hash, after 500/sec, it looks similar to the overhead OTP S/Key for the AODV routing can be called effectively.

5. Conclusion

Mobile Ad-hoc Network exhibits, mobile nodes in dynamic environments which does not establish the network infrastructure such as disaster refers to a router with a network structure that acts on each other hosts. However, the dynamic link structure of the network due to instability and a variety of passive, active attack have been exposed to, there are many security vulnerabilities.

In this paper, the structure via an encrypted session key exchange and security of Mobile Ad-hoc Network routing environment simple and proven safety and effectiveness. Given the growth potential Mobile Ad-hoc Networks are fusion technology is deployed in a variety of fields will be highlighted in a ubiquitous environment. But because of this, This route would require security and authentication technologies highlighted, it will take a lot of effort into the future commercialization of research.

Acknowledgments

This paper is a revised and expanded version of a paper entitled “A Study on Mobile Node Authentication using Encrypted Session Key based on MANET” presented at, C.-S. Lee, Harbin, China, August 19-20 of Proceedings International Conferences NGCIT 2016 and ISI 2016.

This paper was supported (in part) by Research Funds of Kwangju Women's University in 2016 (kwul16-097)

References

[1] B. Kadri, A. M’hamed and M. Feham, “Secured Clustering Algorithm for Mobile Ad Hoc Networks”, International Journal of Computer Science and Network Security IJCSNS, vol. 7, no. 3, **(2007)** Mar., pp. 27-34.

[2] Y.-D. Kim, “Performance of VoIP Traffics over MANETs under DDoS Intrusions”, Journal. of The Korea Institute of Electronic Communication Services, vol. 6, no. 4, **(2011)**, pp. 493-498.

[3] X. Jia, J. Wu and Y. He, “Mobile Ad-hoc and Sensor Networks”, Proceedings Lecture Notes in Computer Science First International Conferences MSN 2005, vol. 3794, Springer, **(2005)**, pp. 164-174.

[4] R. Zheng and R. Kravets, “On-demand power management for Ad Hoc networks”, Twenty-Second Annual Joint Conferences of the IEEE Computer and Communications Societies 2003 (INFOCOM 2003), vol. 1, **(2003)** March, pp. 481-491.

[5] K. Kim, S. Bae and D. Kim, “An Enhanced Robust Routing Protocol in AODV over MANETs”, Journal of The Korea Institute of Electronic Communication Services, vol. 4, no. 1, **(2009)**, pp. 14-15.

[6] C-K Toh, “Ad Hoc Mobile Wireless Networks Protocols and System”, Prentice Hall, **(2004)**, January, pp. 200-252.

[7] Y.-D. Kim, “Transmission Performance of VoIP Traffics over MANETs under Multi Intrusions”, Journal of The Korea Institute of Electronic Communication Services, vol. 7, no. 2, **(2012)**, pp. 258-263.

[8] A. Patwardhan, J. Parker, A. Joshi, A. Karygiannis and M. Iorga, “Secure Routing and Intrusion Detection in Ad Hoc Networks”, Third IEEE Int. Conference on Pervasive Computing and Communications, **(2005)** March.

[9] C.-S. Lee, “A Study on Effectiveness using Security Routing based on Mobile Ad-hoc Networks”, International Journal of Security and Its Applications, vol. 9, no. 7, **(2015)**, pp. 141-152.

[10] V. Boyko, P. MacKenzie and S. Patel, “Provably secure password authenticated key exchange using Diffie_Hellman”, Advances in Cryptology-Eurocrypt 2000, **(2000)** May, pp. 14-18.

[11] C.-S. Lee, “A Study on MD5 Security Routing based on MANET”, Journal of The Korea Institute of Electronic Communication Services, vol. 7, no. 4, **(2012)**, pp. 797-803.

[12] .-S. Lee, “A Study on Mobile Node Authentication using Encrypted Session Key based on MANET”, Proceedings International Conferences NGCIT 2016 and ISI 2016 of Advanced Science and Technology Letters ASTL 138, Harbin, China, **(2016)** August 19-20, pp. 5-9.

Author

Cheol-seung Lee, he is currently an assistant professor at the Teacher Training & Liberal Arts Department at the University of Kwangju women's University in Korea. He received his Ph.D. in Computer Engineering from the University of Chosun, Korea, in 2008.

His recent research activities are focused on Mobile Ad-hoc Network security and Android & iOS programming and privacy in smart environments.