International Journal of Security and Its Applications
Vol.9, No.7 (2015), pp.141-152
http://dx.doi.org/10.14257/ijsia.2015.9.7.13

A Study on Effectiveness using Security Routing based on Mobile Ad-hoc Networks

Cheol-seung Lee

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

Abstract

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 Network has been paid much attention as a Ubiquitous computing which is growing fast in the field of computer science. With performance both as hosts and routers, easy network configuration, and fast response, mobile nodes participating in Mobile Ad-hoc Network are suitable for Embedded 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, hashed AODV routing is used to protect from counterfeiting messages by malicious nodes in the course of path finding and setting, and disguising misrouted messages as different mobile nodes and inputting them into the network.

Keywords: *Mobile Ad-hoc Network, MD5, AODV*

1. Introduction

Although Mobile Ad-hoc Network is suitable for Ubiquitous 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].

This paper suggests that routing security that an AODV (Ad-hoc On-demand Distance Vector) routing protocol is applied to MD5 prove stability and efficiency for routing security of a Mobile Ad-hoc Network. It uses NS (Network Simulator)3 for performance evaluation, retains security about disguise and wiretap of malicious nodes through AODV hashed and proves efficiency through measuring overhead.

2. Mobile Ad-hoc Network Routing and Security Environment

A Mobile Ad-hoc Netowrk 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].

2.1. AODV Routing Protocol

AODV of base of DSDV (Destination Sequenced Distance Vector) supports all of the unicasts and multicasts and uses sequence numbers of a destination node to protect loop. It is able to improve performance of entire networks [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 node [6-7], Also, there is a security vulnerability between the mobile node due to malicious node and compromised mobile node are camouflaged as work normally [8].

ISSN: 1738-9976 IJSIA

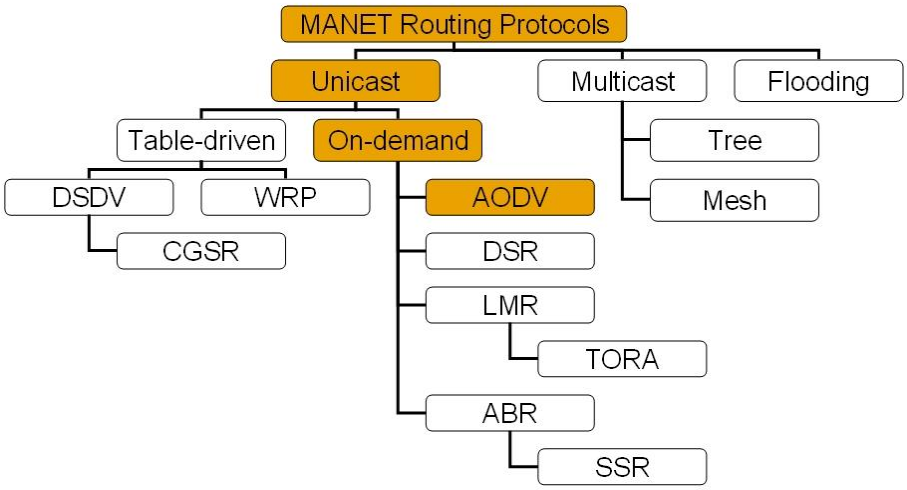

Figure 1. Mobile Ad-hoc Network Routing Protocols

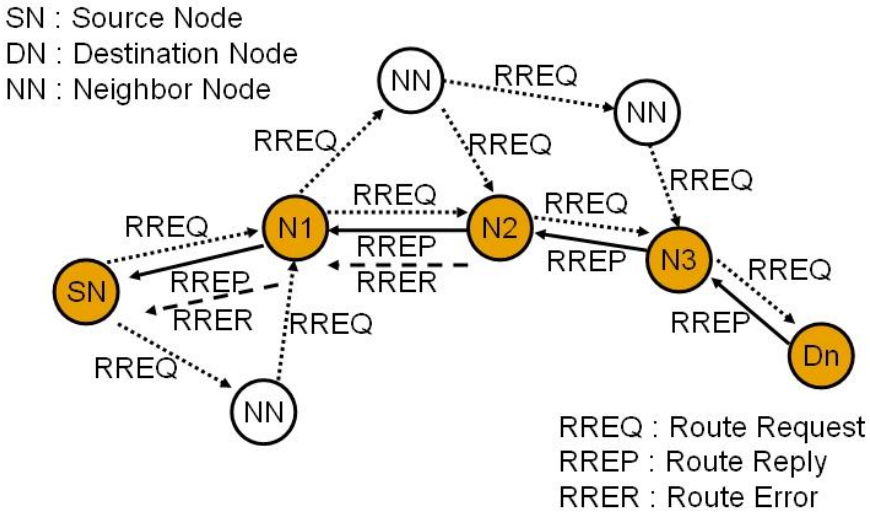

Figure 2. AODV Routing Protocols

As the Figure 2, when a source node would transmit messages for routing to a destination node, it carries out route search unless there is no destination node's routing information and it sends RREQ (Route Request) messages if there is destination node's routing information.

Whenever a neighbor node which received the RREQ message sends sequence numbers and RREQ message, the neighbor node uses broadcast ID and creates own IP address and broadcast ID through address auto configuration method [9].

As a mobile node received the RREQ message send the RREQ message to the destination node, it can set up reverse path due to recording IP address of the mobile node which have sent the first RREQ message to own routing table and the destination node only applies to an link which is the same bidirectional feature because the destination node can answer RREP (Route Response) messages with unicasts way to source node through neighbor node.

The mobile nodes received the RREP message saved as creating forward direction route information, when a mobile node received overlapping the same RREQ message, it uses only the first one received.

If some errors occur in particular link which is in routing route, the mobile node transmit the RERR(Route Error) messages to the source node and launch processing of route re-search [10]. After that, the mobile node received the RERR message deletes routing information related to links which occur errors.

2.2. Security Environment in Mobile Ad-hoc Network

2.1.1. Threat and 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) [7].

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.

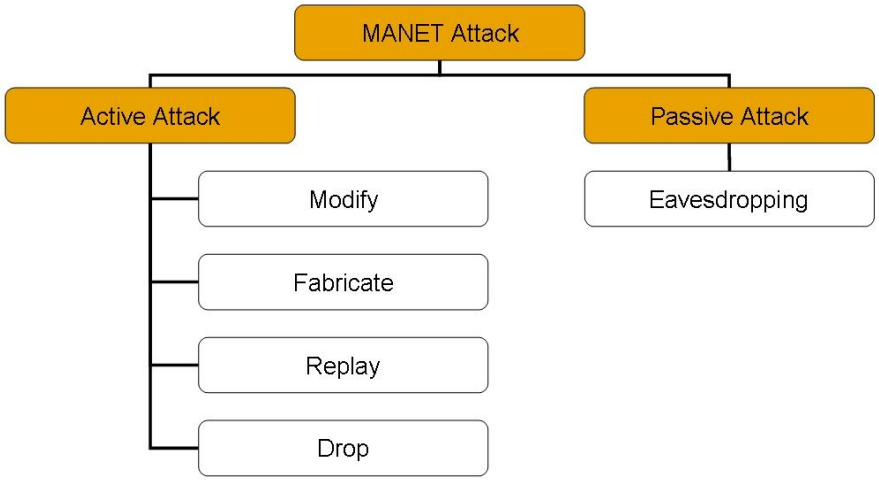

Figure 3. Mobile Ad-hoc Network Attack Pattern

As the Figure 3, The Mobile Ad-hoc Network has active attack and passive attack patterns because it makes the mobile nodes 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 routing technics [8].

2.1.2. MD5 Hash Function: The MD5 provides 128bits random number resulted from the final result value using formula (2.1) from input of variable length. It is used formation of encrypted password using the OTP (One Time Password) and must have protection policy such as inversion, collision and forgery. The inversion is thing that find out a message from hash value is given, the collision is thing that different messages have the same hash value and the forgery is thing that calculate the MAC(Message Authentication Code) without information about secret key. It is used in the wireless device certification standard of IEEE 802.11 and configures

reliable Mobile Ad-hoc Network environment using encrypted password with hash function.

$$A \leftarrow B + ((A + g(B, C, D) + X[k] + T[i]) <<< s) \quad (2.1)$$

Table 1. Parameters in MD5 Hash Function

Parameter	Description
A, B, C, D	MD5 Buffer
g	One of the hash function F, G, H, I
<<< s	Circular left shift by s bits of the 32bit parameter
X[k]	k-th 32bit in the 512bit block of the message
T[i]	i-th 32bit in the matrix T
+	2^{23} addition

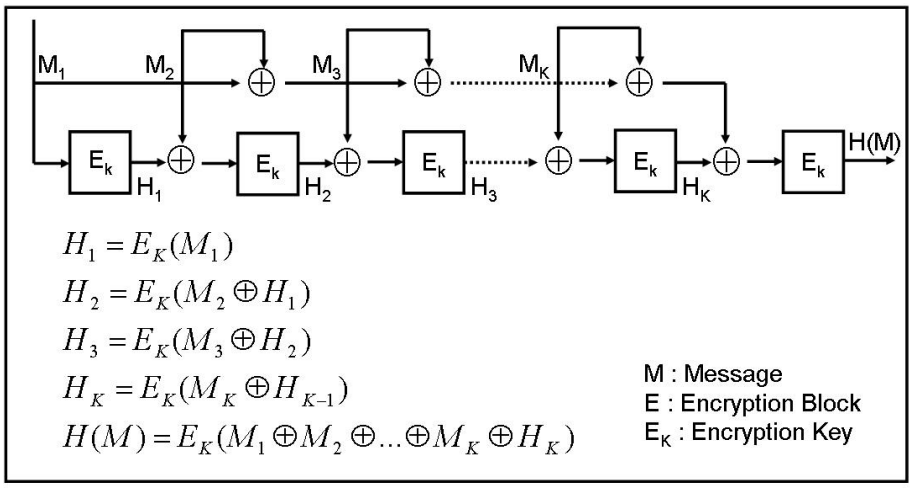

Figure 4. MD5 Hash Function

3. The Security Routing

This paper suggest that analyzing the AODV for security routing and reliable routing technics respond the routing security and the dynamic network topology immediately for route determination.

The mobile node can create 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. Each of the mobile nodes route determination a safe path with confidentiality and integrity through limited security routing [11].

3.1. Security Routing Requirements

The routing protocol study of the Mobile Ad-hoc Network is carried out on the assumption of reliable mobile node but increase an opportunity to be able to do fraudulent acts owing to each of the mobile nodes conducts forwarding, routing and networks' management function.

In case of receiving routing information of the mobile node in particular, the mobile node should be able to determine the ranking in regular sequence of reliability and in case of incorrect routing route determination, the mobile node should be able to delete it for security routing. Also, when it forms a static network topology, it bears high network

overhead because each of the mobile nodes gives and takes touting messages regularly, and needs to have safety regarding impersonation attack of the forgery and spoofing in each field of routing messages among the mobile nodes from malicious nodes.

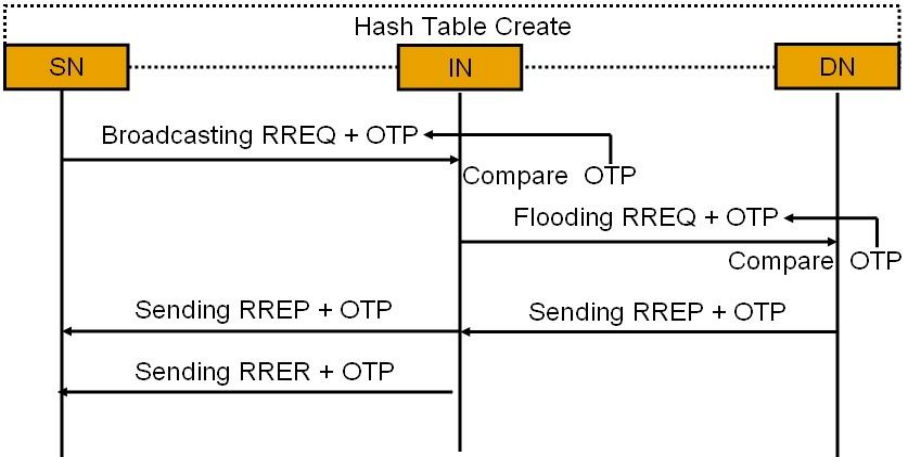

Figure 5. Step of Security Routing

As the Figure 5, it uses the H(AODV) routing protocol combining the OTP into the AODV at the limiting methods' routing step. The OTP certifies routing messages, offers confidentiality and integrity about the forgery of messages from malicious node and sets up routing determination through H(RREQ) and H(RREP) with the hash chain following formation of each of the mobile nodes. It can protecting the hop counter information among mobile nodes and can secure a safe communication path because messages' verification conducts the same method as the OTP digital signature.

3.2 Creation of Hash Tables

A hash tables of mobile nodes create hash chain such as $h^0(x)$, $h^i(x)$, ..., $h^n(x)$ from single bit string x. when i from one to length n, $h^0(x)$ is x, $h^1(x)$ is $h(h^0(x))$ hashed one more and $h^i(x)$ is $h(h^{i-1}(x))$. Each of the mobile nodes makes k numbers' message of n bits using the OTP create hash table.

When each of the mobile nodes j is from one to length n for creating hash tables, they select x_j which is private key factor and create hash chain whose length is k about private key factor of n number.

0	$h^0(x_1)$	$h^0(x_2)$	$h^0(x_3)$	⋯	$h^0(x_j)$	⋯	$h^0(x_n)$
1	$h^1(x_1)$	$h^1(x_2)$	$h^1(x_3)$	⋯	$h^1(x_j)$	⋯	$h^1(x_n)$
2	$h^2(x_1)$	$h^2(x_2)$	$h^2(x_3)$	⋯	$h^2(x_j)$	⋯	$h^2(x_n)$
⋮	⋮	⋮	⋮	⋯	⋮	⋯	⋮
k-t	$h^{k-t}(x_1)$	$h^{k-t}(x_2)$	$h^{k-t}(x_3)$	⋯	$h^{k-t}(x_j)$	⋯	$h^{k-t}(x_n)$
k	$h^k(x_1)$	$h^k(x_2)$	$h^k(x_3)$	⋯	$h^k(x_j)$	⋯	$h^k(x_n)$

Figure 6. Hash Table of Mobile Nodes

The source node transmits a massage after signing it with k-th private key using PKI(Public Key Infrastructure), after adjacent mobile nodes verify the value of $h^k(x_j)$ transmitted from the source node, they make v_j which is one from length n make use of the OTP public key factor of the mobile node.

3.3 Route Determination

For safe route determination, when the source node do a routing to the destination node, the source node transmits route search messages from the intermediate node to the destination node.

As the Figure 7, the source node creates H(RREQ$_i$) guaranteed integrity to apply to *448 mod 512* for signing i-th route searching messages would like to transmit. For signing each bit of the source node's message, it creates one of private key x and one of public key y and $log_2 n$ bit is added to the message. In the H(RREQ$_i$), by calculating zero number of bit strings of message added to the H(RREQ$_i$) and having bit string g of n bit. j-th bit string g_j which is one with respect to all j creates the OTP as formula (3.1) adding H(RREQ$_i$) which find $h^{k-i}(x_j)$ hash value at (k-i)-th line of created hash tables in each the mobile nodes and creates the H(RREQ) transmit the mobile nodes.

$$H(RREQ) = H(RREQ_i) + h^{k-i}(x_j) \quad \text{----------} \quad (3.1)$$

The mobile node received the H(RREQ) message obtains the H(RREQ$_i$) which is applied to the MD5 in order to verification digital signatures and calculates $log_2 n$ and then creates n bit string g value after adding to the H(RREQ$_i$) by calculating zero number of bit strings of message. It should check that j-th bit sting $g_j=1$ with respect to all j is $h^{i-i'}(r_j)=v_j$. the r_j is the OTP of transmitted the H(REEQ) currently and the v_j is H(RREQi')-th OTP.

If $h^{i-i'}(r_j)=v_j$, we can know that integrity of routing information is guaranteed and the mobile node verification the H(RREQ) conducts forwarding procedure repeatedly from the source node to destination node by renewing v_j to r_j values to search and check following H(RREQ).

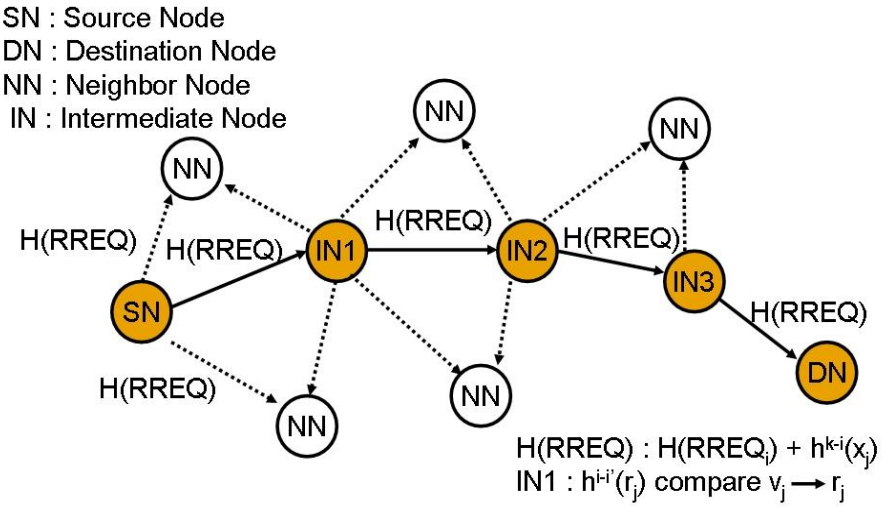

Figure 7. Routing Path Searching

The destination node which receive the H(RREQ) from the source node creates the H(RREP), which is a response message and transmits through reverse path. The H(RREP) makes type sets up two and includes prefix sizes, hob counts of relevant node, IP address of the DN, sequence numbers, IP address of the SN, life time, counter and the OTP of response messages.

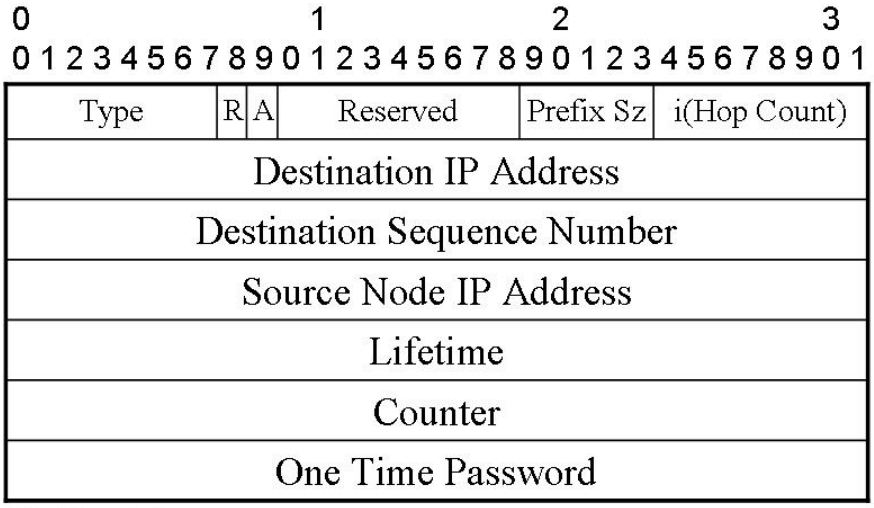

Figure 8. Elements of H (RREP)

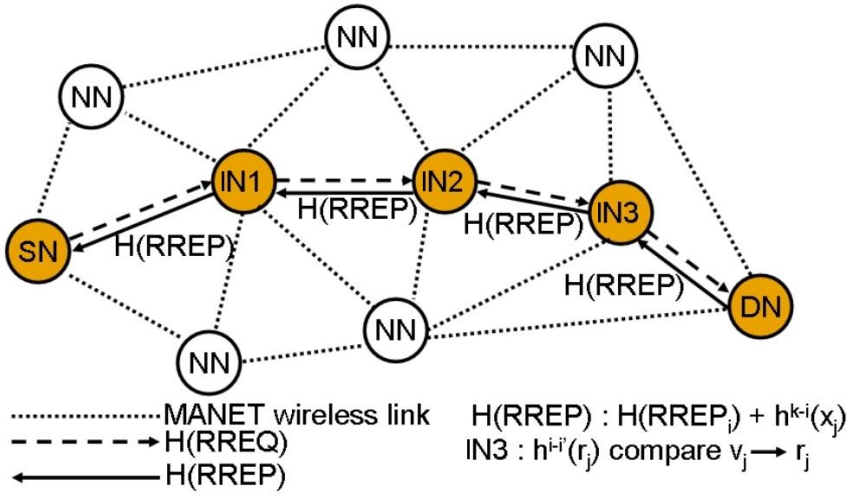

Figure 9. Routing Path Setting

As the Figure 9, the IN3 received *i*-th H(RREP$_i$) of the destination node creates the OTP as the same way of the H(REEQ) and integrity is guaranteed by verifying digital signature.

$$H(RREP) = H(RREP_i) + h^{k-i}(x_j) \quad \text{----------} \quad (3.2)$$

The IN3 verifying the H(RREP) makes v_j renew r_j values and carries out forwarding procedure repeatedly from the IN3 to the source node to search and verify following the H(RREP). Therefore, we can make malicious node which disguised as another node do not spread incorrect routing information or prevent regeneration attack about the H(RREP) to secure a safe routing path.

Type = 1 //H(RREQ)
Hop Count = 0
Broadcast ID += 1
Destination IP Address
Destination Sequence Number = Last Destination Sequence Number
Source IP Address
Source Sequence Number = Last Destination Sequence Number + 1
One Time Password

Type = 2 //H(RREP)
Hop Count = 1 //Destination Node
Hop Count = Destination Hop + 1 //Intermediate Node
Destination IP Address
Destination Sequence Number = last Destination Sequence Number + 1 //Destination Node
Destination Sequence Number = last Destination Sequence Number //Intermediate Node
Source IP Address
Lifetime = Routing Effective Time
One Time Password

Figure 10. H (AODV) Path Setting Process

After route determination, each of the mobile nodes transmits confirmation messages regularly to the mobile nodes to check valid routing path. Unless mobile nodes happen traffic of path during life time, it checks that the path does not act on a routing table.

However, if the data is transferred from invalid path or path link is cut off, it transmits generated the H(RRER). We can prevent a malicious node which is disguised as formal mobile node from attack of generating the H(RRER) because the H(RRER) is signed as the OTP.

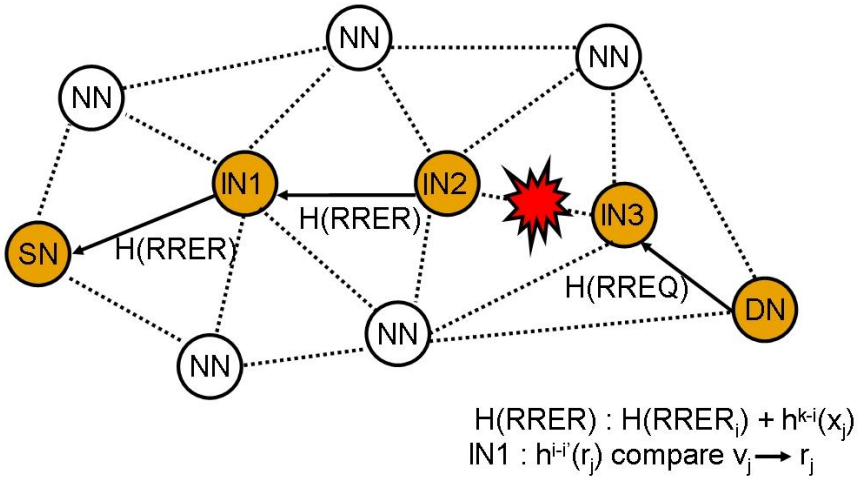

Figure 11. Routing Error

4. Experiments and Results Analysis

4.1. Experimental Environment

Table 2. 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 2, 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.

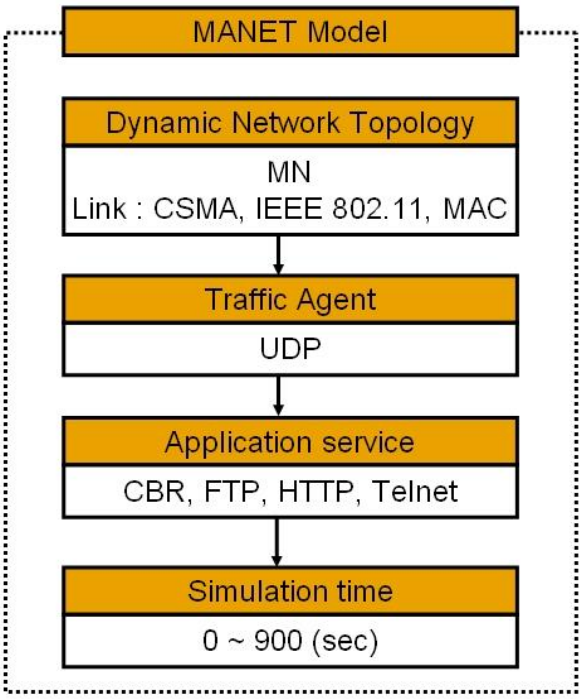

Figure 12. Design of Mobile Ad-hoc Network

4.1.2. Evaluation: Hop counters between the mobile nodes and message fields are not altered because the suggestion technic uses formula (3.1) and (3.2). If routing massages are altered by malicious node participating networks, it is tracked out by the intermediate node and offers integrity due to deleting transmitted message.

When a routing massage take part in networks, it has difficulty in distinguishing attack pattern through forged message because only the mobile node which makes own public

key transmit another mobile node. However, the suggestion technic can know the mobile node sends forged routing message through public key that malicious node signed so it can exclude malicious node and not act as a forging of legal mobile node later on routing process.

4.2. Efficiency Analysis

4.2.1. Packet Delivery Fraction: The packet delivery fraction measurements compared Suggested technic with AODV. Source node is first started the CBR 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.

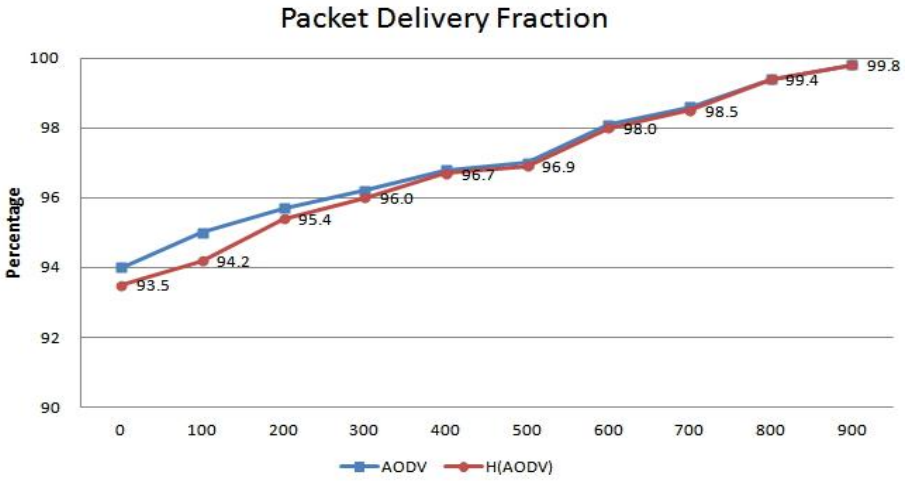

Figure 13. Packet Delivery Fraction

$$\textit{Packet delivery fraction} = (\textit{receive\_packet} / \textit{send\_packet}) * \frac{}{100} \quad \text{----- (4.1)}$$

Figure 13 is the generated result value by cbrgent.tcl. If the down-time is zero, the mobile node moves to the destination node and transmits only the H(RREQ) and H(RREP) message inserting OTP without additional message process to routing protocol.

The AODV demonstrates packet delivery fraction over 94% during simulation, also the suggestion technic shows similar delivery fraction. But packet transmission ratio declines for route search beside the AODV when a simulation starts as 93.5%. However, it can show gradual increase in packet transmission ratio after 400 sec, it notifies that searching and setting up route for transmitting and receiving data packets is efficient and accurate compare to suggestion technics is 99.8% and the AODV are seen 0.1% error at 900 sec.

4.2.2. Routing Overhead: Routing overhead is the number of taken control packets during the CBR session that one of the data packets transmitted from the source node to destination node. When the data should be transmitted from the source node to destination node, used message occurs in agent level, routing level and MAC level, the massage of agent level is the CBR data which would like to transmit, the message of routing level is a RTR_level message for transmitting the CBR data, the message of the MAC level is address determination protocol message and measured routing overhead linked to 30 numbers' nodes out of 50 nodes participating in the network.

As the Figure 14, the AODV has 1.71 numbers' routing packets for routing searching, the suggestion technic has 2.30 numbers' routing packets; much bigger routing packet than the AODV has is transmitted. But it shows as similarly as the AODV routing packet after 500 sec so it can be efficient.

Routing overhead=(MAC_level_messages+RTR_level_messages)/receive_messages ----- (4.2)

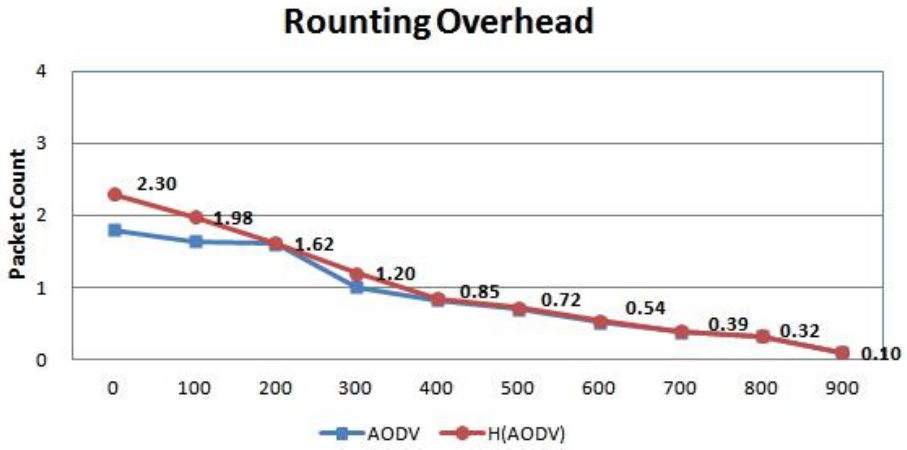

Figure 14. Routing Overhead

5. Conclusion

The Mobile Ad-hoc Network is the network which is able to transmit and receive data with routing performing between the mobile nodes in an environment which has no infrastructure construction as an existing network. But it has numerous security vulnerabilities such as link stability, physical preservation limitation of the mobile node and link dispersibility of the mobile node compare to wired network as a dynamic network topology result from mobility of the mobile node.

In this paper, simple structure, safety and efficiency are proven using the OTP which applies to the MD5 for security routing of a the Mobile Ad-hoc Network environment. If the Mobile Ad-hoc Network growth is considered, security consciousness of the Mobile Ad-hoc Network will increase geometrically and a routing technic will be the most necessary thing. If the ubiquitous environment and the Mobile Ad-hoc Network's marketability are considered, highlighted routing protocol, a development of security technic and a commercialization study will be needed.

Acknowledgement

This paper was supported (in part) by Research Funds of Kwangju Women's University in 2015.

References

[1] B. Kadri, A. M'hamed and M. Feham, "Secured Clustering Algorithm for Mobile Ad Hoc Networks", J. International Journal of Computer Science and Network Security, vol. 7, no. 3, (**2007**), pp. 27-34
[2] A. Sahu and V. Sejwar, "Improved Trust Based Routing Mechanism in DSR Routing Protocol in MANETs", J. International Journal of Future Generation Communication and Networking, vol. 8, no. 1, (**2015**), pp. 137-148
[3] X. Jia, J. Wu and Y. He, "Mobile Ad-hoc and Sensor Networks", Proceedings of the Lecture Notes in Computer Science First International Conference MSN 2005, vol. 3794, Springer, Wuhan, China (**2005**).
[4] Q. Liu, N. Linge and F. Gao, "Towards Context Exchange in a MANET Environment", J. International Journal of Future Generation Communication and Networking, vol. 5, no. 2, (**2012**), pp. 61-70.

[5] C. S. Lee, "A Study on MD5 Security Routing based on MANET", J. Korea Institute of Electronic Communication Services, vol. 7, no. 4, (**2012**), pp. 797-803.
[6] C. K. Toh, "Ad Hoc Mobile Wireless Networks Protocols and System", Prentice Hall, New Jersey (**2002**).
[7] Y. D. Kim, "Transmission Performance of VoIP Traffics over MANETs under Multi Intrusions", J. International Journal of Future Generation Communication and Networking, 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 International Conference on Pervasive Computing and Communications, (2005) March 8-12; Kauai Island, Hi.
[9] K. Weniger and M. Zitterbart, "Address autoconfiguration in mobile ad hoc networks: current approaches and future directions", IEEE Journals & Magazines, vol. 18, no. 4, (**2004**), pp. 6-11.
[10] M. G. Zapata and M. Guerrero, "Secure Ad Hoc On-Demand Distance Vector (SAODV) Routing", IETF Internet Draft: draft-guerrero-manet-saodv-05.txt, (**2005**).
[11] C. S. Lee, "A Study on Effective Hash Routing in MANET", Proceedings of the 3rd International Conference on Computer, Information and Application, (2015) May 21-23; Yeosu, Korea.

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.

