Advanced Science and Technology Letters
Vol.95 (CIA 2015), pp.47-54
http://dx.doi.org/10.14257/astl.2015.95.10

A Study on Effective Hash Routing in MANET

Cheol-seung Lee

Dept. of Teacher Tranining & Liberal Arts, Kwangju Women's University
201 Yeodai-Gil, Gwangsna-Gu, Gwangju, Korea
cyberec@kwu.ac.kr

Abstract. Recently demands in construction of the stand-alone networks and interconnection between convergence devices have led an increase in research on and much attention has been paid to the application of MANET as a Ubiquitous network which is growing fast. With performance both as hosts and routers, easy network configuration, and fast response, mobile nodes participating in MANET are suitable for Embedded computing, but have vulnerable points, such as lack of network scalability and dynamic network topology due to mobility, passive attacks, active attacks, which make continuous security service impossible. 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: MANET, MD5, AODV

1 Introduction

A MANET (Mobile Ad-hoc Networks) has been demonstrating high growth of Ubiquitous computing applications. However, MN(Mobile Node)s presenting in a MANET have been studying under mutual dependence and have been target of an attack of malicious nodes owing to incompletion of routing security [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 MANET. It uses NS3 for performance evaluation, retains security about disguise and wiretap of malicious nodes through AODV hashed and proves efficiency through measuring overhead.

ISSN: 2287-1233 ASTL

2 MANET Routing and Hash Function

2.1 AODV Routing Protocol

AODV [3],[4] of base of DSDV(Destination Sequenced Distance Vector) supports all of the Unicasts and Multicasts and uses sequence numbers of a DN(Destination Node) to protect loop. It is able to improve performance of entire networks.

When a SN (Source Node) would transmit messages for routing to a DN, it carries out route search unless there is no DN's routing information and it sends RREQ (Route Request) messages if there is DN's routing information. Whenever a NN (Neighbor Node) which received the RREQ message sends sequence numbers and RREQ message, the NN uses broadcast ID and creates own IP address and broadcast ID through address auto configuration method [5].

As a MN received the RREQ message send the RREQ message to the DN, it can set up reverse path due to recording IP address of the MN which have sent the first RREQ message to own routing table and the DN only applies to an link which is the same bidirectional feature because the DN can answer RREP(Route Response) messages with Unicasts way to SN through NN. The MNs received the RREP message saved as creating forward direction route information, when a MN 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 MN transmit the RERR messages to the SN and launch processing of route re-search [6]. After that, the MN received the RERR(Route Error) message deletes routing information related to links which occur errors.

2.2 MANET Threat and Attack Pattern

The MANET is short of physical defense about malicious nodes from unsafety links, limited frequency, transmission distance, energy limitation between MNs and interference of electric wave resulted from increase in the MN. 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 MANET 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 MN provides incorrect information for the MNs 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 MN with the sufficient MNs. The MANET has active and passive attack patterns because it makes the NNs transmit data through multi hop. Also, the MNs compromised malicious nodes look like working normally but, they might distort the networks of routing structure so it exists security weakness between the MNs and needs reliable MANET security routing technics [8].

2.3 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 MANET environment using encrypted password with hash function.

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

- A, B, C, D : MD5 buffers
- 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

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. After it makes first set of the public key is used digital signature apply to the MD5 repetitively and creates hash tables, it leads to a lot of sets of the public keys' elements from hash tables at the routing stage. Each of the MNs route determination a safe path with confidentiality and integrity through limited security routing.

3.1 Security Routing Requirements

The routing protocol study of the MANET is carried out on the assumption of reliable MN but increase an opportunity to be able to do fraudulent acts owing to each of the MNs conducts forwarding, routing and networks' management function [9].

In case of receiving routing information of the MN in particular, the MN should be able to determine the ranking in regular sequence of reliability and in case of incorrect routing route determination, the MN 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 MNs 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 MNs from malicious nodes.

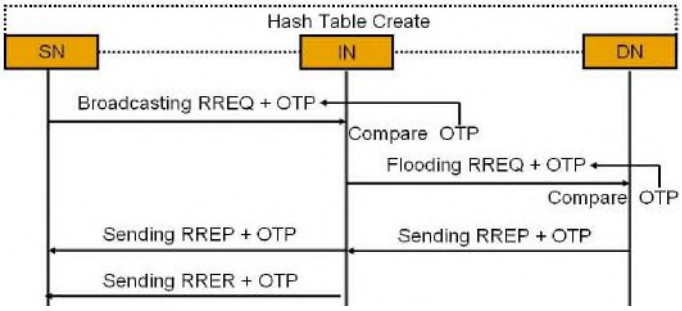

Fig. 1. Step of Security Routing.

As the Fig. 1, it uses the H(AODV) routing protocol combining the OTP into the AODV at the limiting methods' routing stage. 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 MNs. It can preserve hop counter information among MNs 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

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-i	$h^{k-i}(x_1)$	$h^{k-i}(x_2)$	$h^{k-i}(x_3)$	⋯	$h^{k-i}(x_j)$	⋯	$h^{k-i}(x_n)$
k	$h^k(x_1)$	$h^k(x_2)$	$h^k(x_3)$	⋯	$h^k(x_j)$	⋯	$h^k(x_n)$

Fig. 2. Hash Table of MNs.

As the Fig. 2 hash tables generate 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 MNs makes k numbers' message of n bits using the OTP generate hash table. When each of the MNs j is from one to length n for generating hash tables, they select x_j which is private key factor and generate hash chain whose length is k about private key factor of n number. The SN transmits a massage after signing it with k-th private key using PKI(Public Key Infrastructure), after adjacent MNs verify the value of $h^k(x_j)$ transmitted from the SN, they make v_j which is one from length n make use of the OTP public key factor of the MN.

3.3 Route Determination

For safe route determination, when the SN do a routing to the DN, the SN transmits route search messages from the IN(Intermediate Node) to the DN. the SN 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 SN'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.

As the Fig. 3, 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 sting g_i which is one with respect to all *j* generates the OTP 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 MNs and makes the H(RREQ) transmit the NNs.

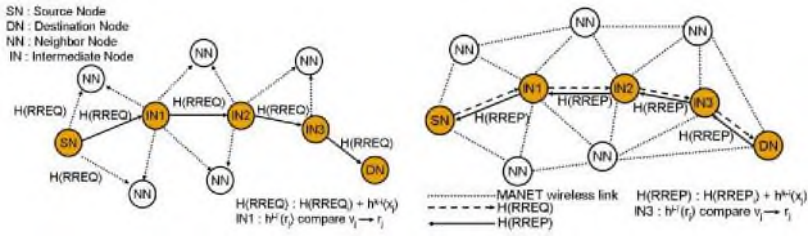

Fig. 3. Route Determination.

The NN 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 0 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 MN verification the H(RREQ) conducts forwarding procedure repeatedly from the SN to DN by renewing v_j to r_j values to search and check following H(RREQ). The DN which receive the H(RREQ) from the SN 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.

The IN3 received *i*-th H(RREP$_i$) of the DN creates the OTP as the same way of the H(REEQ) and integrity is guaranteed by verifying digital signature. The IN3 verifying the H(RREP) makes v_j renew r_j values and carries out forwarding procedure repeatedly from the IN3 to the SN 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.

After route determination, each of the MNs transmits confirmation messages regularly to the MNs to check valid routing path. Unless MNs 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 MN from attack of generating the H(RRER) because the H(RRER) is signed as the OTP.

4 Performance Evaluation

The MANET model is made up using the NS3 for performance evaluation of suggestion technics. Firstly, according to IEEE 802.11 link layer and the TDMA(Time Division Multiple Access), traffic agents of the MN and application services are decided by the CSMA(Carrier Sense Multiple Access) using the MN 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, fourth course sets up simulation time from 0~900(sec) and measures overhead about the $n/log_2 n$ packet.

If routing massages are altered by malicious node participating networks, it is tracked out by the IN 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 MN which makes own public key transmit another MN. However, the suggestion technic can know the MN 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 MN later on routing process.

4.1 Packet Delivery Fraction and Routing Overhead

Compare to the AODV and the suggestion technic, the measure of packet delivery is that the SN starts the CBR session generates packets of four 512byte/sec and it measures transmitted data packet up to the DN according to the MN's movement (0 – 20m/sec) using random waypoint, computational complexity and delay time.

Fig. 4 is the generated result value by cbrgent.tcl. If the down-time is zero, the MN moves to the DN 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.

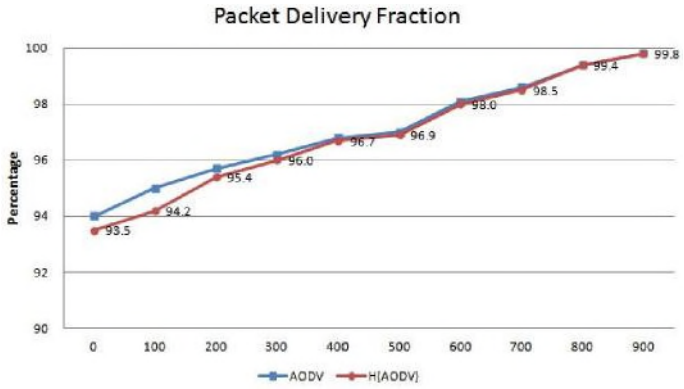

Fig.4. Packet Delivery Fraction

Routing overhead is the number of taken control packets during the CBR session that one of the data packets transmitted from the SN to DN. When the data should be transmitted from the SN to DN, 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.

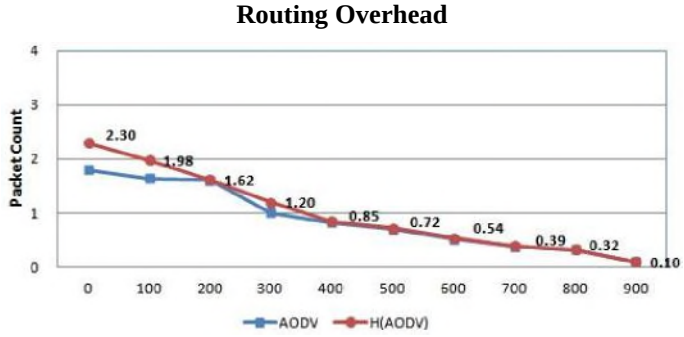

Fig.5. Routing Overhead.

As Fig. 8 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.

5 Conclusion

The MANET is the network which is able to transmit and receive data with routing performing between the MNs 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 MN and link dispersibility of the MN compare to wired network as a dynamic network topology result from mobility of the MN.

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

References

1. B. Kadri, A. M'hamed, M. Feham, "Secured Clustering Algorithm for Mobile Ad Hoc Networks", IJCSNS International Journal of Computer Science and Network Security, vol. 7, no. 3, pp. 27, (2007)
2. Y.-D. Kim, "Performance of VoIP Traffics over MANETs under DDoS Intrusions", J. of The Korea Institute of Electronic Communication Services, vol. 6, no. 4, pp. 493-498, (2011)
3. M. S. Corson, J. P. Macker, "Mobile Ad hoc Networking(MANET) : Routing Protocol Performance Issues and Evaluation Considerations", RFC 2501, pp. 3-5, January, (1999)
4. C.-S. Lee, "A Study on MD5 Security Routing based on MANET", J. of The Korea Institute of Electronic Communication Services, vol. 7, no. 4, pp. 797-803, (2012)
5. K. Weniger, M. Zitterbart, "Address autoconfiguration in mobile ad hoc networks : current approaches and future directions, "IEEE Netw. Mag., vol. 18, no. 4, pp. 6-11, (2004)
6. Manel Guerrero Zapata, Manel Guerrero, "Secure Ad Hoc On-Demand Distance Vector (SAODV) Routing", IETF Internet Draft : draft-guerrero-manet-saodv-05.txt, pp. 12-13, (2005)
7. C-K Toh, "Ad Hoc Mobile Wireless Networks Protocols and System", Prentice Hall, pp. 200-252, (2004)
8. A. Patwardhan, J. Parker, A. Joshi, A. Karygiannis, M. Iorga, "Secure Routing and Intrusion Detection in Ad Hoc Networks", Third IEEE International Conference on Pervasive Computing and Communications, pp.2-3, (2005)
9. G. Montenegro, C. Castelluccia, "Statistically Unique and Cryptographically Verifiable (SUCV) Identifiers and Address", NDSS' 02, pp. 1-2, (2002)

