ACSIJ Advances in Computer Science: an International Journal, Vol. 4, Issue 6, No.18 , November 2015
ISSN : 2322-5157
www.ACSIJ.org

ACSIJ
WWW.ACSIJ.ORG

A Secure and Efficient Routing Protocol with Genetic Algorithm in Mobile Ad-hoc Networks

Atieh Moghaddam[1], Ali Payandeh[2]

[1] Computer Department, University of Tehran, Company
Tehran, IR.TE, Iran
a.moghaddam@alumni.ut.ac.ir

[2] ICT Department, Malek-e-AshtarUniversity, Company
Tehran, IR.TE, Iran
payandeh@mut.ac.ir

Abstract

Routing in Mobile Ad-Hoc Networks (MANETs) is a challenging task due to its nature of open medium, infrastructure-lessness, dynamicity and no trusted central authority. In MANET, a node can be compromised during the route discovery process. Attackers from inside or outside can easily exploit the network. Several secure routing protocols have been proposed for MANETs. In this paper, Ad-Hoc On-Demand Distance Vector (AODV) routing protocol is considered due to the fact that it uses the shortest number of wireless hops towards a destination as the primary metric for selecting a route with independence of the traffic congestion. To add security to AODV, Secure AODV was designed to enhance security services to the original AODV. Secure AODV protocol has been designed with cryptographic techniques such as digital signatures and hash chains, which can have a significant impact on the routing performance of AODV routing protocol. To improve efficiency of SAODV, Enhanced SAODV (ESAODV) was proposed based on Genetic Algorithm and alternative path. The genetic algorithm optimizes the routes in terms of selected metrics. The performance and impacts of using AODV, S-AODV and ESAODV routing protocols were compared using NS-2 Simulator. The simulation results demonstrated that using the proposed mechanism could significantly decrease the End-to-end delay and routing overhead.

Keywords: *Mobile ad-hoc network, SAODV routing protocol, genetic algorithm, end-to-end delay, packet routing overhead.*

1. Introduction

Mobile ad-hoc network is a collection of nodes that are connected to each other with wireless links without any infrastructure. The routing protocols in ad-hoc environment can be classified as proactive routing protocols and reactive routing protocols. Proactive protocols maintain whole paths in routing tables and when the source node wants to establish a route to the destination node, the path that already exists in its routing table is used. In reactive protocols, the route is established only when the source node needs to send a data packet to the destination. There are varieties of routing protocols for MANET such as AODV, DSR, OLSR …, but none of them are secure. As a result, they assume there is no malicious node in the network; however, due to the flexibility of the MANET, there are a lot of vulnerabilities in this kind of network and security problem is the most significant issue in it. Two different security mechanisms are presented for routing protocols. The first one guarantees authentication and integrity of the routing messages. The second mechanism allows node to control another node behavior during route discovery process. Both two approaches need some network resources such as battery, energy and bandwidth. The main purpose is finding the balance between efficiency and security.

The remaining part of this article is organized as follows. Section 2 describes SAODV routing protocol. Section 3 introduces genetic algorithm briefly. A proposed routing protocol is given in section 4. And section 5 shows the simulation results.

2. SAODV Routing Protocol

The first secure and promoted version of AODV is secure AODV (SAODV) that is based on asymmetric cryptography. In SAODV protocol, the routing messages (RREQ, RREP, and RERR) are encrypted by digital signature to guarantee the integrity and authenticity. Due to not propagating the RREQ for external nodes, this routing protocol prevents from external active attacks. All nodes are authenticated by a unique password. When a source node wants to send the RREQ, it first authenticates its neighbors by that password and then broadcasts the message. In SAODV, the sender signs the routing

messages by its private key and the receiver verifies them by the sender's public key. Because of incrementing the hop-count in each step of routing discovery, the sender cannot encrypt it. Hence, for securing this field (that is, not allowing malicious node to reduce it), SAODV uses hash chain.

This structure is difficult to use when an intermediate node has a path to destination in routing table since RREP necessarily has to have destination signature. For solving this problem, SAODV uses double signature. In this mechanism, RREQ has a second signature that is always stored with the reverse path route. An intermediate node, which wants to reply RREQ, uses second signature and adds it to RREP. Then it is sent to the source node. The RREQ and RREP messages fields are:

<Type, Length, Hash function, Max-hop-count, Top Hash, Signature, hash>

The RERR message fields:

<Type, Length, reverse, Signature>

When a node creates RREQ or RERR, It does the functions as follow:

1. Generate a random number (seed)
2. Max-hop-count = timeToLive
3. Hash = seed
4. Hash-function = h
5. Top-hash = $h^{max\text{-}hop\text{-}count}$ (seed)

Verifying hop-count in RREQ or RREP by intermediate node:

1. Top-hash = $h^{max\text{-}hop\text{-}count}$ (Hash)

Update hop-count, apply hash to generate new hash chain, then send it to all neighbors.

However, SAODV messages are significantly larger and require heavy computation because of digital signature, especially for double signature.

SAODV solves the overhead of routing tables by updating them in particular time. So SAODV prevents the black hole attack. In comparison with AODV, due to an encryption in SAODV, malicious node cannot access the content of the messages; nevertheless cryptography process increases routing delay and the length of the messages.

3. Genetic Algorithm

Finding the shortest path in mobile ad-hoc networks requires the evaluation of route from the source to the destination, which has the least cost. The old algorithms such as Dijkstra and Bellman ford present how the shortest path is found. Yet, these algorithms are especially used for wired network and are not suitable for wireless networks. Genetic algorithm is one of the algorithms that are useful for ad-hoc networks and it is used for designing more effective protocols.

John Holland proposed genetic algorithm in 1970. The route consists of sequence of nodes. This algorithm executes on routes, which are achieved from route discovery process. In the first step, the path is coded by sequence of integers, which these are the node's IP. The length of this sequence cannot be more than the number of nodes. GA operation consists of six necessary levels: genetic presentation, initial population, fitness function, selection, crossover and mutation. This collection is "standard GA" (SGA).

3.1 Genetic Presentation

The path is coded by sequence of integers, which are node's IP.

3.2 Initial Population

Each chromosome shows a potential solution. Initial population consists of numbers that represents the chromosomes in AODV protocol. The routes that are achieved from route discovery process are intended for initial chromosomes.

3.3 Fitness Function

The quality of each solution should be evaluated accurately. In this function, the main purpose is finding the richest path between source and destination. The fitness parameters are described according to the problem requirements. In this paper, the goal of using genetic algorithm is finding the shorter path from the source node to the destination node with reducing end-to-end delay.

3.4 Selection

This function plays the significant role to promote the average of population quality by selecting the high-qualified chromosome for next generations. Selection is operated on fitness output. Each chromosome that has the best fitness value is selected. This function plays the

significant role to promote the average of population quality by selecting the high-qualified chromosome for next generations. Selection is operated on fitness output. Each chromosome that has the best fitness value is selected.

3.5 Crossover

Crossover processes the current solutions to find the better approach. In this process, one or more than a bit of chromosome changes and a new population is created. Genes are selected from father's chromosomes and make the new children.

3.6 Mutation

GA could fast access the demanded level of cost. Mutation randomly changes some bits of sequences and move them to new location of existing solution.

4. Proposed Protocol

In this paper, ESAODV is proposed to improve the efficiency of SAODV. ESAODV eliminates the same routing messages, uses genetic algorithm to find the better path in route discovery and also saves an alternative path and uses it when the link failure occurs.

To preserve the security in this protocol, similar to SAODV, digital signature and hash chain are used. This mechanism prevents ESAODV from external attack, eavesdropping and black hole attack.

4.1 Propagation RREQ and RREP

When the source node needs a route to the destination, it creates RREQ and broadcasts it to all neighbors. Intermediate node receives the RREQ packet and then checks the routing table. If there is a route to the destination with higher sequence number, this intermediate node sends the RREP to the source by reverse path. Otherwise, each intermediate node updates its routing table and then sends the RREQ to all neighbors until the destination receives the message.

During the execution of this process, some nodes may give the same RREQ many times and broadcast it more than once, which reduces the energy of nodes and increments the delay. The new mechanism has been designed in ESAODV to prevent from responding the same routing message. When the node receives the RREQ for the first time, it saves its broadcast IP in the routing table. After that, whenever it receives the RREQ with the same IP, it does not broadcast this message because it is reiterative. This solution causes reduction of routing delay and saves the energy of nodes.

As shown in figure 1, A is a source node and 1, 2, 3, 4 and 5 are intermediate nodes. A Broadcasts RREQ to all neighbors and it continues by others. Node 3 is a neighbor of 1 and 2. So it receives RREQ from both 1 and 2 and broadcasts the same RREQ twice.

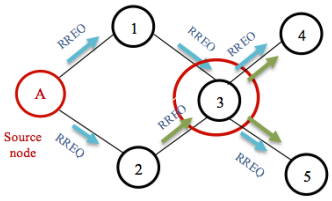

Fig. 1 Broadcasting RREQ in SAODV.

In ESAODV, when node 3 receives the RREQ for the first time, it saves its broadcast IP. After that, whenever it receives the RREQ, firstly it checks the routing table. If the current IP is similar to the IP that exists in routing table, the node eliminates the same RREQ and does not broadcast it. Otherwise, the message is broadcast to its neighbors.

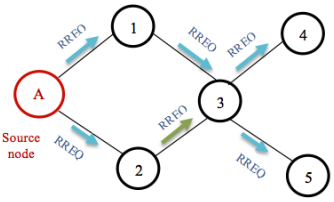

Fig. 2 Broadcasting RREQ in ESAODV.

In the proposed protocol, this structure has also been implemented for broadcasting the RREP. B is the destination node and 4, 5, 6, 7 and 8 are the intermediate nodes.

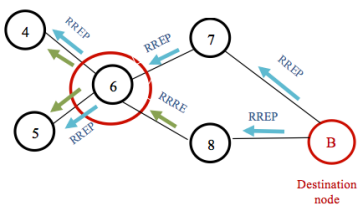

Fig. 3 Broadcasting RREP in SAODV.

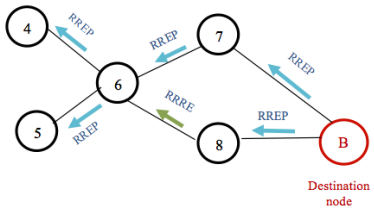

Fig. 4 Broadcasting RREP in ESAODV.

4.2 Implementing the Genetic Algorithm

In the routing process, finding a route, which has less delay, is an important challenge. Smart algorithm is a kind of algorithm that is used in optimization problems to find the better solution. Genetic is one of the smart algorithms that evaluate the chromosome according to the purpose.

In ESAODV, genetic algorithm is executed after the route discovery process. The routes that are found from this process create initial population. Fitness of this algorithm is calculated based on the delay. Each RREQ message has timestamp, which shows the time of the message creation. Route delay is the difference between routing current time (the time that message is received by the destination) and RREQ timestamp.

$$rdelay = (CURRENT\_TIME - rq\_timestamp) \quad (1)$$

rdelay is a variable that shows the delay. Current_time is a time that the message is received by the destination. rq_timestamp is a time that the RREQ has been created. According to the calculated delay for each path, the path that has the least delay is selected. So not only is the rout selected based on the hop-count, but also delay affects selecting it. Genetic algorithm both speeds the routing process and finds the better route to send the data. Due to the reduction of the delay, the network lifetime is increased.

4.3 Alternative Path

After executing route discovery and genetic algorithm, the output of algorithm is selected as a current route to send the information. If link failure occurs, route discovery process in SAODV begins again. This approach increases the packet routing overhead.

ESAODV uses an alternative path. In this mechanism, the second path is saved in routing table of the nodes. When the genetic algorithm is done and the better path is selected for sending the data, the second better path (which has the least delay except the first rout) is selected as an alternative path. So when the link failure occurs, the second path alternates the current route and sending the information continues. To implement this mechanism, each node has rt-count function. This function shows the number of the path to the destination. If this number is less than one, the second path is saved as an alternative path. During the execution of the protocol, if the route with less delay is found, this route is changed with the alternative path and the routing tables are updated. This approach significantly minimizes the packet routing overhead.

5. Simulation Results

NS2 simulator is used to illustrate the performance of the proposed protocol. In this simulation, AODV, SAODV and ESAODV are compared. Table 1 shows the simulation parameters.

Table 1: Simulation parameters

Simulation Time	120 s
Simulation Area Size	1000 * 1000 m
Number of Nodes	30
Data Transfer Rate	4 Packet /s
Wireless nodes transfer scope	250 m
Data packet size	512 bytes
Mobility mode	Random
Packet transfer speed	1-10 mb/s
Traffic model	CBR

5.1 Packet Delivery Fraction

The ratio of the number of data packets received at the destination to the number of those originated at the source.

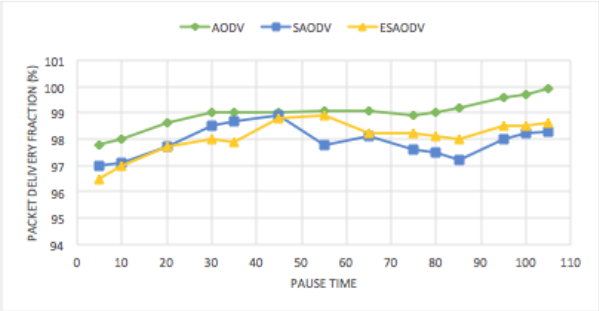

Fig. 5 Packet Delivery Fraction Diagram.

5.2 Average End-to-End Delay

End-to-end delay represents the time that it takes the packets to be received by the destination. Due to the cryptographic techniques in SAODV and ESAODV, average end-to-end delay is more than AODV.

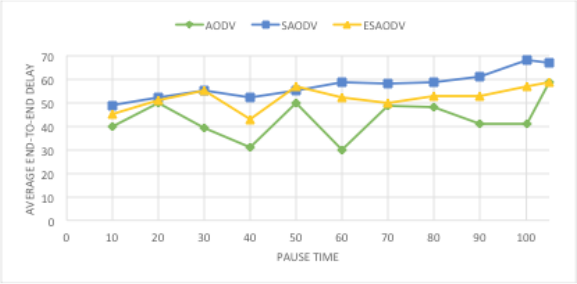

Fig. 6 Average end-to-end delay diagram.

5.3 Number of dropped packet

This parameter represents the number of the dropped packets.

Dropped packet = send packets – receive packets

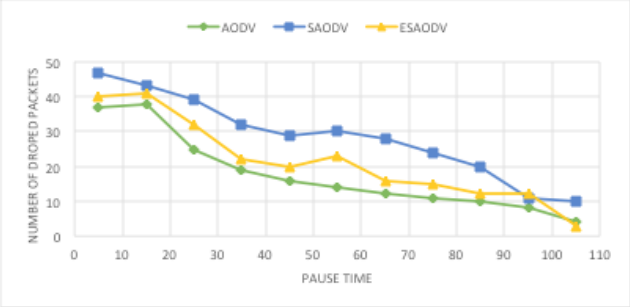

Fig. 7 Number of dropped packet diagram.

5.4 Packet routing overhead

The ratio of the data packet to the number of the routing packets that have been sent.

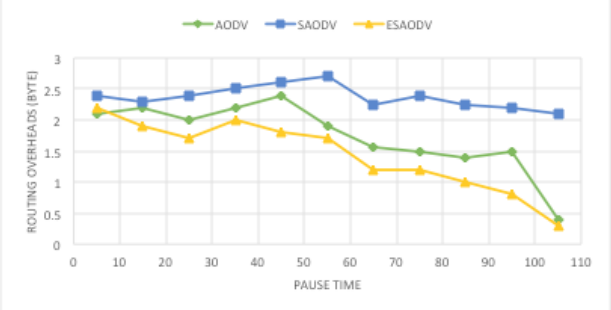

Fig. 8 Packet routing overhead diagram.

Table 1 shows the advantages and disadvantages of some secure routing protocols and the proposed protocol.

Table 2: Advantage and Disadvantage of Secure Routing Protocol and ESAODV

Secure routing protocol	***Prevent from***	***Advantage***	***Disadvantage***
ARAN	Change, Eavesdropping, Impersonation	Easy to implement	Expensive, vulnerable to wormhole
SAR	Change	Dynamic routing, cost	Not always shortest path
SRP	Detection and prevention of impersonated packet	Prevent from eavesdropping	Vulnerable to change and wormhole

SEAD	Change the transferred routing information	Effective use of cpu and energy	Vulnerable to wormhole
ARIADNE	Change, impersonate the routing information	Prevent from wormhole	Abandon malicious node
ESAODV	Change, eavesdropping, black hole	Authenticating the node	Need more storage resources

6. Conclusions

To increment the performance of the network, ESAODV uses the technique in which the intermediate node does not respond to the same RREQ and RREP messages. Also, the fitness function of the genetic algorithm is designed based on minimum delay to find the better path from the source to the destination. Additionally, alternative path prevents from beginning the route discovery process when the source node receives the RERR message. All these mechanisms remarkably decrease the end-to-end delay and the packet routing overhead of the networks.

References

[1] M.Manjunath, D.H. Manjaiah, "Comparative Study of AODV, SAODV, DSDV and AOMDV Routing Protocols in MANET Using NS2," in International Conference on Computing and Intelligence Systems, , March 2015, vol. 4, special issue, pp. 1174-1180.

[2] G. Cerri, A. Ghioni, "Securing AODV: The A-SAODV secure routing prototype," Communications Magazine, IEEE , vol. 46, no. 2, 2008, pp. 120-125.

[3] J. Rajeshwar, Dr. G. Narsimha, "A Comparative Study on Secure Routing Algorithms SAODV and A-SAODV in Mobile Ad-hoc Networks (MANET)- The Enhacements of AODV," International Journal of Computers and Technology, vol. 3, no. 2, 2012, pp. 419-424.

[4] T. R. Andel, "Surveying Security Analysis Techniques in MANET Routing Protocols," IEEE Communications Survey, The Electronic Magazine of Original Peer-Reviewed Survey Articles, vol. 9, no. 4, 2007, pp. 70-85.

[5] J. Neeli, Dr. N.k. Cauvery, "Comparative Study of Secured Routing Protocols in Wireless Ad hoc Networks: A Survey," International Journal of Computer Science and Mobile Computing, vol. 4, no. 2, February 2015, pp. 225-229.

[6] A. k. Mishra, B. D. Sahoo, "A Modified Adaptive-SAODV Prototype for Performance Enhancement in MANET," International Journal of Computer Applications in Enineering, Technology and Sciences (IJ-CA-ETS), vol. 1, no. 2, 2009, pp. 443-447.

[7] A. Banerjee, "Administrator and Trust Based Secure Routing in MANET," in Advances in Mobile Network, Communication and its Applications (MNCAPPS), 2012 International Conference on, 2012.

[8] A. Sharma, M. Sinha, "Influence of crossover and mutation on the behavior of Genetic algorithms in Mobile Ad-hoc Networks," Computing for Sustainable Global Development (INDIACom), International Conference on. IEEE, 2014, pp. 895-899.

[9] J.H. Holland, Adaptation in Natural and Artificial, in The University of Michigan Press, USA, 1975.

[10] D. Suresh Kumar, K. Manikandan, M.A. Saleem Durai, "Secure on-demand Routing Protocol for MANET Using Genetic Algorithm," International Journal of Computer Applications, vol. 19, no. 8, April 2011, pp. 29-35.

[11] E. Baburaj, V. Vasudevan, "An Intelligent Multicast Ad-hoc On demand Distance Vector Protocol for MANETs," Journal of Networks, vol. 3, no. 6, June 2008, pp. 62-69.

[12] P. Gaur, "An Efficient Routing Implementation Using Genetic Algorithm," International Journal of Computer Science and Mobile Computing (IJCSMC), vol. 2, no. 7, 2013, pp. 250-257.

[13] P. Singh, G. Singh, "Security issues and link expiration in secure routing protocols in MANET: a review," International Journal of Advanced Research in Computer and Communication Engineering, vol. 3, no. 7,July 2014, pp. 7559-7565.

Atieh Moghaddam is completed the Bachelor of Science in software engineering in 2010. She completed the Master of Science in information security from Tehran University in 2013. She is a member of network Security Company. Her area of interest spans Genetic Algorithm, security issues in mobile ad-hoc networks and cryptography.

Ali Payandeh received B.Sc. and M.Sc. degrees in electrical engineering From Tarbiat Modarres University, Iran, in 1991 and 1994, respectively, And the Ph.D. degree in electrical engineering from K. N. Toosi University of Technology, Iran, in 2006. From 1991 to 1995, he was a faculty member in the Department of Electrical engineering at Malek-e-Ashtar University of technology, Iran. Since 1996, he has been a Director of Research at the Applied Science Research Association (ASRA), Iran, where he has involved in research for secure satellite communications. His research interests include information theory, coding theory, secure communications and satellite communications.