Authenticated Hierarchy Double Signature protocol for MANET

Ali Bagherinia[1], *Nik Mohammad Balouchzahi*[2], Ali Jowharpoor[3], Sohrab Hojatkhah[4]

[1]Islamic Azad university- Dehdasht branch

Abstract

In this paper we present a secure routing protocol based on reliability hierarchy levels and using reliable server. Reliable server grants certifications to authenticated nodes in MANET. Simulated results shows when there is intruder nodes packet delivery ratio of proposed method is greater than delivery ratio of other related method such as AODV and DSR. In contrast packet dropped ratio resulted from presented method is less than other method. Whereas end to end delay for each node in proposed method is higher than other method, but in first all data quicker reach to destination node.

Keywords: *MANET, Routing, Security*

1. Introduction

1.1 Background *of MANET*

Ad hoc network are 72 age approximately. First they are created for military goals, for example military fighter and their mobile database in battle field. Later commercial and industrial usages of them were discovered. They consist of removable and distributed nodes that without central manager build a temporary network.

MANET can stereotype in two groups:[1]

First: Sensor network: they consist of sensor which have located in specified geographical range. Each sensor has abilities such as wireless connectivity, enough intelligence for signal processing and network potential.

Second: Wireless Ad hoc networks: they are defined as revocable users that connect with each other via wireless links. Because central networks aren't effective for unforeseen events and aren't reliable hence MANET is suitable solution for such environments. In wireless Ad hoc networks each node is equipped with wireless sensor and receiver and broad casting /peer to peer Antenna. Now days MANET using is increased incredibly such as: Military environment, emergency functionality, science and explorer environment.

MANET has particular property such as:

- Platform less; these network don't require central and integrated structure similar sensors, routers, etc, therefore often used mechanism for them is based on assistance of all nodes.

- Using wireless connection: main cause of flexibility and accessibility these networks.

- Multi hope: In these networks nodes play router role. Therefore a packet passes through multi nodes to reach destination.

- Irregular relocation of nodes: leads to hardship routing and topology changing. Each node may be out of access at a time and as soon next time be accessible in network.

- Resource limited: you note that mention nodes have enough memory, processing strict constraints in contrast constant nodes.

1.2 Security in Networks

Network security is specified as "we reliable that intrude people couldn't access to secret message and couldn't manipulate them". Source of security problem are people that try to gain other attention or harmful to other. Hence security achievement is bigger than program bug correction [2]. MANET security services don't compare to other network security services. Goal of security is information and resources protection from malicious node attacks.

For achieving suitable and correct performance, below condition must be preferred:

- Availability: if network services are require any time they are exists in spit being attack. Availability satisfier systems search denial of service (DOS) attacks, energy starvation attacks and ill-behaved of nodes. Such as selfish at packet communication.

- Authentication: satisfy of connection between two networks must be reliable and pure; on the other words a malicious node couldn't nominate itself as authenticate node in network.

- Confidentiality: is satisfied that a message couldn't distinguishable for each node else destination node. This satisfaction us usually is done by symmetric/asymmetric data encryption.

- Integrity: correction and authentication of sending data; if node A sends a message to B, other nodes between A and B such as C couldn't change this message. By using strong security mechanism data validation is simple as inserting a one way hashing before message encryption [3].

- Non- repudiation: satisfy that a node couldn't repudiate its generated message. One solution for this is using digital signatures.

1.3 Network Routing

To go to points and feasibility of security isn't concentrate in particular point. Therefore we must consider security cases for each layer of network architecture. For example in physical layer by create a connection from wire and eavesdrop on cable access to other people information is possible. To prevent from such attack we can put cable into pipe with full gas. When other wants to create unauthorized connection, gas is discharge and alarm will be active. This is a mechanical approach and for other layer logical approaches are used.

Routing protocol is very important for all networks, but wireless routing protocol is completely differing from wired networks. Wired routing protocols aren't responsible for managing of node motion in network. Also isn't necessary try to decreasing node connection overhead, because wired networks have large bandwidth. These protocols will been encountering routers that they are reliable.

One of the MANET properties is node motion. Also for designing MANET routing protocol resource constraints play an important role, in added all nodes must participate in routing hence routing protocol don't execute on reliable entity (strict routers). Therefore distinguish MANET routing protocol must be designed. This is a research field for network researchers in these years.

This paper is organized as: we discuses related work at section 2. We proposed a new security approach at section 3. Simulated results and conclusion are shown in 4, 5 sections in order.

2. Related Work

2.1 SAODV

The secure version of AODV is known as SAODV [4, 5]. This protocol has specification such as integrity, acknowledgement. This algorithm uses 2 methods: firstly, each node should signature its created message. This method cause other nodes identify message creator. This method protects constant field of Rout Request and Response messages. But these message has a hop count field because that is variable first method couldn't protect it. Therefore another method is considered that protects variable fields of a message. Second method uses hash chain idea [6].

For signature routing message it's necessary that different nodes must have a key pair for using a symmetric cipher. In addition each node in network should aware from other nodes certificated public keys. Therefore network needs a key management scheme [7].

SAODV adds extension to AODV message to provide security goals. Each node that receive a message, firstly checks certification of message signature. Generally this method work correctly for AODV. In contrast it has a constraint. In AODV protocol all nodes that received request message if have new route can reply to this message.

This method increase total utilization of routing detection process and decrease generated overhead. But by using digital signature in SOADV, this useful property can't usable. Because intermediate nodes can't generate routing reply message only target nodes can generate these message. For solving this problem a double signature method is suggested for SAODV protocols [8].

There are a lot for danger attack to this algorithm one of them, is when a node received a routing request message don't increase hop count field. There for hash field hasn't changed and other nodes can't detect this malicious behavior. One other attack is: malicious node repeats hashing process of hash value and increase hop count multi time. In addition SAODV protocol can't resist against wormhole attacks.

Other attacks that SAODV can't prevent them are as follow: A node dropped routing message and decrease protocol utilization. Other attack is a node that doesn't need to know the route sends infinite frequent request and increase protocol overhead and saturated other nodes process and discharge their batteries. To oppose these attack IDS systems can be used with SOADV protocol [9].

2.2 DSR Protocol

DSR is an inaction protocol [10]. This protocol uses source routing method. It has two main parts, route detection and route maintenance. Route detect process is for nodes that connect to particular destination but they don't knew each route to destination. Route maintain

process is for detect routes that by moving or insurability of nodes are destroyed.

Because nodes move continuously in MANET and link between nodes may be destroyed. DSR protocol does this mechanism by using receiving acknowledgment in MAC layer. For more detail see [11].

3. Proposed Algorithm

Each node has two Puk1 and Puk2 public key. A GS server is considered for network that is reliable that generate distribute initial reliability degree of nodes. All nodes in network access to public key of GS server and can checks other nodes validation. Each node such as A has two certification as: $cert_A = [IP_A, PuK1_A, t, e]PrK_T$ that is primary certification and $Scert_A = [IP_A, PuK2_A, t, e]PrK_T$ second certification .In them IPA is IP address of A, $PuK1_A$ is first public key of A and $PuK2_A$ is second public key of A, t is certification generating time and e is certification expire time. Also PrK_T declares that this certification is signature by private key of GS server.

A reliability hierarchy is considered for network nodes that initial reliability degree is specified by GS server. Each application that needs to security preferably sends and receives packets only via reliable nodes and avoid from sending packets through the shortest route that may contains unreliable node(s).

In each sending route request message process if intermediate nodes (between source and destination) if have a r eliable route to destination. They can reply to source. Permission delegation of destination signature is done by using Puk2.

Executing of this algorithm is as follows:
When a node (suppose A) want to find a route to a destination (suppose X); first propagate a routing finding packet (RFP) in network. This message has a $[[\mathrm{RFP}, \mathrm{IPx}, \mathrm{Cert_A}, \mathrm{N_A}, \mathrm{t}, Scert_A, \mathrm{RQ\_SEQ\_REQIR}, \mathrm{RQ\_SEQ\_}GAR]\ \mathrm{PrK_A}]$ format. In this format: RFR is type of message (Route Request), IP_X is IP address of X, $\mathrm{Cert_A}$ is primer certification of A, NA is current value of A that is incremented one step after A sends each message, t is current time, $\mathrm{SCert_A}$ is secondary certification of A, RQ_SEQ_REQIR is required security level for requested route and RQ_SEQ_GAR is maximum granted security level of each node for requested route. Then "RFP message is signature with private key of A. When other node (such as B) receive this message if it can't guarantee need reliable level of source (that is extracted from RQ_SEQ_REQR) this node drop out this message else via extracting $PuK1_A$ from $\mathrm{cert_A}$ checks the message and if the message is valid, B checks message signature also checks t (for identify of time expiration). After this check, if the message is valid, B creates a route to source of the RFP message (A) in opposite direction of received message route. Then B save $\mathrm{SCert_A}$ (because, after this message if B has reliability degree for received RFP to A destination, B reply them).If B node know request route of RFP) and if it has secondary certification of X ($\mathrm{SCert_X}$) it reply to RFP source (A) instead of X (send a RRP and don't propagate received RFP from A in network. Else B don't have requested route of RFP or don't have secondary certification of X ($\mathrm{SCert_X}$) with its private key and attaché its primary certification ($\mathrm{Cert_B}$) to receive RFP and propagate it for its neighbor as follow format $[[\mathrm{RFP}, \mathrm{IP_x}, \mathrm{cert_A}, \mathrm{N_A}, \mathrm{t}, Scert_A, \mathrm{RQ\_SEQ\_REQIR}, \mathrm{RQ\_SEQ\_}GAR]\ \mathrm{PrK_A}]\ \mathrm{PrK_B}, \mathrm{cert_B}$. When next node (such as C) received this RFP message does similar process such as B. But if B needs to propagate received RFP, it replaces $\mathrm{Prk_B}$, $\mathrm{Cert_B}$ with $\mathrm{Prk_C}$, $\mathrm{Cert_C}$ and propagates a m essage as $[[\mathrm{RFP}, \mathrm{IP_x}, \mathrm{cert_A}, \mathrm{N_A}, \mathrm{t}, \mathrm{RQ\_SEQ\_REQIR}, \mathrm{RQ\_SEQ\_}GAR]\ \mathrm{PrK_A}]\ \mathrm{PrK_C}, \mathrm{cert_C}$ for its neighbors.
Finally destination node of A RFP message (X) received this message and checks their validation and certification, if RFR is satisfied checks conditions, it replies to RFP message with format as: $[\mathrm{RRP}, \mathrm{IP_A}, \mathrm{cert_X}, \mathrm{N_X}, \mathrm{t}, RQ\_SEQ\_REQIR, RQ\_SEQ\_GAR]\ \mathrm{prk_X}$. In this message; RQ_SEQ_GAR is copied from RQ_SEQ_GAR in received RFP and declares maximum guaranty security level of route. Node X does signature RFP message with its private key ($\mathrm{Prk_X}$). When C node received RRP message, if C can't guaranty needed reliability level for message sender (X) (that is appear via EQ_SEQ_REQID, it drop out RRP packet. Else check its certification, if it is validated, it s aves RQ_SEQ_GAR as its security level. At last C signature RRP and attached its certification ($\mathrm{Cert_C}$) and send it to previous node (B node). Other nodes repeat this process until RRP reaches to route requester node (B node). Finally node A receive RRP, check its certification and if RRP is valid, the A starts data sending to X.

4. Simulation

Simulation was done with SWANS [12]. Nodes are placed randomly in area with 1000*1000 m^2, with propagation range 150m, speed of each node between 0 through 20 m/s. Packet delivery and packet drop out are considered as achievement parameters. We consider 1 to 5 nodes from 25 nodes as malicious. Simulation result of packet deliver ratio is shown in Fig.1 and packet drop is shown simulation Fig.2.

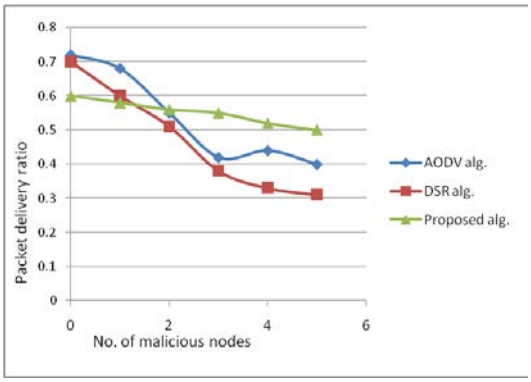

Fig. 1 Packet delivery ratio again malicious nodes

5. Conclusion

To being security in MANET presented simulation shows that proposed algorithm is suitable for a network that there is probability of malicious scrambler and network load is not very busy. But in conditions that packet dropping decreasing and packet delivery is increasing is more important than delay of reaching packet to destination, proposed algorithm is useful. Therefore proposed algorithm is useful. Hence proposed algorithm is suitable for conditions such as: security is important or all data must reach to destination quickly inspect much delay for each packet.

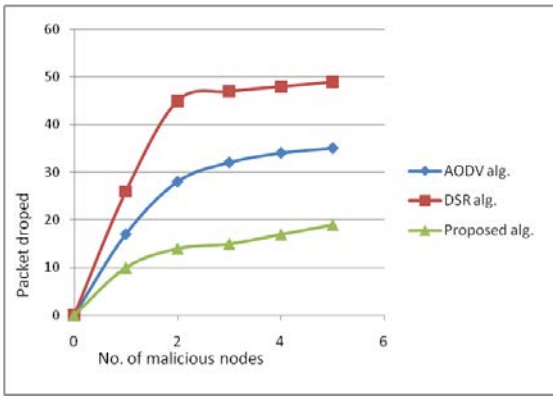

Fig. 2 packet dropped again malicious nodes

References

[1] Christian Tshudin, Per Gunningberg, Henrik Lundgren, Erik Nordstrom, Lessons from experimental MANET research, Computer Science Department, University of Basel, Switzerland, IT Department, Uppsala University, Sweden, 17 August 2004.

[2] Andrew S. Tanenbaum, Computer Networks, fourth edition, Prentice Hall publication.

[3] W. Stallings, Cryptography and Network Security Principles and Practices,3ed.,Pearson EducationInc.,2003.

[4] Manel Guerrero Zapata, "Draft-guerrero-manet-saodv-02.txt", http://ietfreport.isoc.org/idref/draft-guerrero-manet-saodv/.

[5] M. G. Zapata and N. Asokan, "Securing Ad hoc Routing Protocols," WiSe, September 2002. Engineering Institute, CERT Coordination Center, October 2000.

[6] K. Sanzgiri, B. Dahill, B. N. Levine, C. Shields, and E. M. Belding-Royer, "A Secure Routing Protocol for Ad hoc Networks," in International Conference on Network Protocols (ICNP),2002.

[7] Farooq Anjum, Petros Mouchtaris, "Security for Wireless Ad Hoc Networks", John Wiley & Sons, Inc., Publication, 2007.

[8] M.G. Zapata and N. Asokan, "Securing Ad hoc Routing Protocols", WiSe, September 2002.

[9] John McHugh, Alan Christie, and Julia Allen, "The Role of Intrusion Detection Systems", Software Engineering Institute, CER Coordination Center, October 2000.

[10] D. B. Johnson et al., "The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks (DSR)," IETF Draft, draft-ietf-manet-dsr-10.txt, July 2004.

[11] Mohammad Al-Shurman, Seong-Moo Yoo, Seungjin Park, " Black Hole Attack in Mobile Ad Hoc Networks", Proceeding of the 42nd annual southeast regional conference ACM-SE 42, April 2004.

[12] http://www.corel.edu.