Authentication Process Using Secure Sum for a New Node in Mobile Ad Hoc Network

Praveen Gupta and Pratosh Bansal

1 Introduction

Wireless MANETs are deployed by using many independent nodes. These nodes are self-organized nodes. The network has nodes with high mobility. Nodes communicate either directly (when they are in the communication range) or indirectly (using intermediate nodes for data forwarding). MANET can be created at the time of requirement. These networks can easily be established in such areas or situations, where deployment of a wired network is not feasible. With these advantages, a MANET has several disadvantages like node transfers data over an open channel, highly mobile nature of node requires up-to-date location information, nodes are having less computing resources like processing power, less battery power, lesser bandwidth, and may have short life span [1–4].

These features make a MANET more vulnerable. A malicious node tries to access resources without permission. It is the responsibility of the network establisher to design a network with security features. Some MANET does not need high-level security while some may need high security [5]. It depends on the situation for which a MANET is deployed.

Rest of the paper is covered in the following sections. Section 2 describes the security issues in mobile ad hoc network. Section 3 is a literature review. Section 4 explains the proposed algorithm, result, and analysis of results. Section 5 concludes the work.

P. Gupta (✉) · P. Bansal
Information Technology, IET, Devi Ahilya Vishwavidyalaya, Indore, MP, India
e-mail: praveen.gupta@live.com

P. Bansal
e-mail: pratosh@hotmail.com

R. K. Shukla et al. (eds.), *Data, Engineering and Applications*,
https://doi.org/10.1007/978-981-13-6351-1_7

2 Security Issues in Mobile Ad Hoc Network

Various attacks are possible in MANET. Attacks may occur either from inside or from outside of the network. An intruder is either part of the system or a stranger. It compromises legitimate nodes to get the information [6]. The format of their attack is to access information or data actively or passively. In passive format, an attacker only listens to floating information. In active format, an attacker steals information and either deletes or modifies it. In all the cases, tampering or loss of any data is crucial to complete the goal for which MANET is set up [7]. Sometimes these attacks are done to choke the network activities so that network can be unavailable to its users. This can be done by sending many requests to a genuine node and keep it busy to reject other service requests. It is termed as Denial of Service (DoS) attack [4, 8]. A malicious node does packet flooding in the network and all other nodes waste their resources in the processing of these packets. Many such DoS attacks like jamming, packet injection, blackhole, wormhole, etc., are possible in the network. In some other attacks, malicious node targets routing information. They misguide other nodes in the network by providing false, old or modified route details.

All security features: privacy, authentication, integrity, non-repudiation, and availability cannot be achieved at once. Each system has its pros and cons. Various techniques have been proposed by researchers for the security breaches. Security measures can be applied at all levels of the network. Security measures can be applied either as preventive measures or as reactive measures. It is better to have preventive security measures in the network to avoid the attacker's initial attempt to get the entry or to access the resources in an unauthorized manner.

This paper is focused on one of the security feature authentications to prevent unauthorized entry of node in network and access to resources. Though a legitimate user in the network may get compromised later and perform malicious activities. Authentication in a network assures entry of genuine node. Various ways are used to allow a node in the network. A node can show its credentials and gets an entry in the network. It is easily possible in wired and planned wireless network. For an unplanned mobile ad hoc network, authentication mechanism should be devised in such a manner that it does not put a load on network activities and does not require additional devices.

3 Literature Survey

Security issue in a MANET is a critical issue. The major question is how and where to apply security measures to create a fully protected network. Researchers have contributed their work on various types of attack and their countermeasures. In the newborn stage of MANET, researchers were paying attention to general problems

like resources availability, channel limitation, and routing issues. Threats were classified in two classes, viz., attacks and misbehavior. Routing attacks like modification, impersonation, fabrication are possible in the network. Authentication, neighbor detection, and its monitoring are some major solutions [1, 2]. Attacks in the MANET were classified as external and internal, attacks at protocol stack layer, cryptographic primitive attacks. Encryption and authentication are the preventive mechanisms and the intrusion detection system is a reactive mechanism [3, 5].

MANETs are used for such situation where quick set up of a wired network is not possible. The set up of MANET also needs security protocols accordingly [7]. Wireless MANET can be deployed using various types of devices. It can be designed in various forms like mesh networks, sensor network, vehicular network, etc. All these networks share common properties of MANET and face common security problems [4, 6].

Secure communication in any network is a challenging job. Authentication is one of the preventive mechanisms that can be achieved by either using encryption or Public Key Infrastructure (PKI), such things need additional set up of special nodes. Authentication can be done in the limited area using key exchange program. It uses the pre-authentication concept to prove the identity of each other in a small area located network [9].

MANET can be developed for its communication between available nodes or it can be developed with a network that connected with the Internet. For this, it requires two levels of authentications, level 1 for the network working without the internet. The node present at one hop count distant of each other and level 2 authentication for a network with the Internet is used when it has a centralized server [10].

The same level of security cannot be achieved in a MANET as available in the wired network. Environmental situations, where network deployed, also give its impact on network working. It raises the question of Quality of Services (QoS) [5, 11]. Major two security factors, authentication, and confidentiality provide high security to a MANET. These factors may be affected by limited resources, node mobility, and no central control nature of MANET. Some techniques for authentication are symmetric cryptography, asymmetric cryptography, threshold cryptography that requires huge resources for computation. Similarly, confidentiality can be attained by using symmetric, asymmetric encryption, and stream cipher [12].

The methods suggested by researchers need additional infrastructure, a centralized server in case of PKI, and extra resources to run heavy encryption algorithms for authentication. This paper concentrates on developing an algorithm that does not need extra infrastructure or resources for short-span unplanned MANETs.

4 Proposed Algorithm

Generally, a MANET is always set up in a situation where users do not have enough time to deploy the wired network. The main implementation area of a MANET is an emergency situation. The life span of such a network is very less. It is crucial for an

administrator to set up the network with the full plan instead it is important to send readily available nodes to start the work.

Network security is the major concern during its deployment. A MANET is vulnerable to security threats. Threats are ranging from various types of attacks like unauthorized access to network resources, data modification, data deletion, etc. It is required here to secure the flow of information in the network.

A mischievous node tries to obtain floating information either for itself or to deliver it to other nodes. Initially, it is almost impossible to say which node is legitimate or unlawful. There are various ways to save the network from threats. The best preventive mechanism is to restrict such node at the entry level. Authentication of a new node at the entry point of network assures that only legitimate node will work in the network.

The current work proposes an algorithm to authenticate a new node. The algorithm is named as Algo_Authenticate_Node. The main assumptions for this algorithm are: It is designed for small life span of the MANET. It is devised for an unplanned MANET that is deployed for rescue operations like the flood, fire, earthquake, etc. Small life span networks also include conference or meeting. The MANET can start with the minimum of three "key" nodes. These key nodes are used for the authentication process. Other nodes can also be deployed for other tasks.

4.1 Algorithm details

This algorithm uses the minimum of three key nodes for authentication. Each node is assigned a large number. Any key node does not have knowledge of what number is assigned to the other two nodes. A secured "sum" (it is the sum of three large numbers) is given to every key node.

When a new node wants to join the network, it must contact the nearest key node. The key node will provide a number to new node, which is the sum of its own large number and a random number "r" (only known to key node). The new node will go to the next available key node and give this sum to it. Next key node will add its own large number to sum and give the new sum to the new node. The same process is done by the third key node.

New node gives the total sum to again the first key node. The first key node will minus the random no "r" from the total sum. If the remaining value is equal to "sum" then the new node has cleared its authentication process and it can be allowed on probation to participate in networks initial activities.

Algorithm Description:

Algo_Authenticate_Node

This algorithm authenticates the request of a node N_a by method secure sum. Assuming key nodes K_i are at least three.

Algo_Authenticate_Node

Step 1: Start;
Step 2: go to key node 1;
Step 3: r=random ( ); //generates a random big number
sum = r;
Step 4: for i = 1 to n;
{
sum = sum + k_{ir}
}
Step 5: go to node 1;
Step 6: sum = sum-r;
Step 7: if sum != $\sum_{i=1}^{n} k_i$
then
discard the node
otherwise
insert the node
Step 8: Stop;

Advantages of the algorithm: first, it does not require many nodes for authentication. The network must have minimum 3 key nodes for authentication. (If two nodes can be used they may easily guess the opponent number). Even, number of nodes will increase the authenticity in the network; second, it is lightweight algorithm and does not require heavy resources and time to compute the process. Third, it is used for a network of a short-span time period. Fourth, it is difficult to guess the individual number as well as the secured sum. Fifth, the algorithm takes three large numbers, which is not possible to break in a short span of time.

The above algorithm has its limitations. First, it is used for short lifetime of the network. Second, if anyone of the key node dies, authentication activity stops. Third, for high mobility of the node, a new node may have to wait to get a response from the key node.

Working: It is assumed that a node may take variable time for authentication process it is denoted by T_{min}, T_{avg}, and T_{max}. It is also assumed that when a new node sent a request to the nearby key node, a key node gives the response to its request in the time limit of 0.1 to 1 ms.

Table 1 Processing time for authentication [key nodes = 3]

Number of new nodes for processing	Avg process time = T_{avg} (in ms)	Number of nodes	Total time = T_{avg} *nodes (in ms)
P10	1.571	10	15.71
P20	1.629	20	32.58
P30	1.75	30	52.5
p40	1.752	40	70.08
p50	1.651	50	82.55
p60	1.7	60	102
p70	1.557	70	108.99
p80	1.724	80	137.92
p90	1.768	90	159.12
p100	1.732	100	173.2

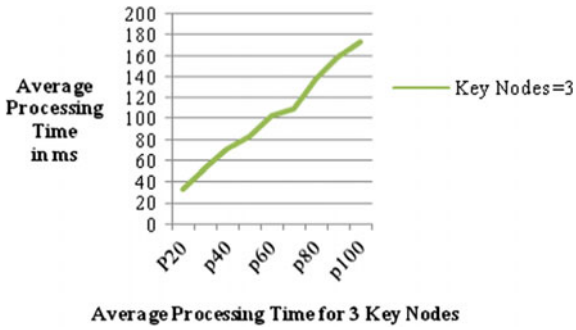

Fig. 1 Average processing time by 3 key nodes

Each key node will process authentication request within this time limit. The given below tables are created for 3 key nodes. Table 1 is comprised of columns that have values for a number of new nodes wants to enter into the network. This range is from 10 to 100. Next column gives the average processing time taken by 3 key nodes for the authentication process of one node in the range of 10–100 nodes. The last column gives the total average time taken for all nodes of a group or range, i.e., 10–100.

Initially, the analysis is done by keeping the number of key nodes fixed whereas the number of new nodes varies from 10 to 100. Figure 1 gives the average processing time taken by three key nodes, where the number of new nodes varies from 10 to 100. Figure 2 gives the comparative chart for average processing time taken by key nodes (3–6) for the group of 10–100 new nodes. In another variation where the number of new nodes is kept fixed, i.e., 50 and key nodes vary from 3 to 6. Figure 3 gives the average processing time for a given combination. From the above figures, it is observed that the time taken by key nodes for varying new nodes is almost linear in nature. It can say that average processing time is proportional to the number of nodes.

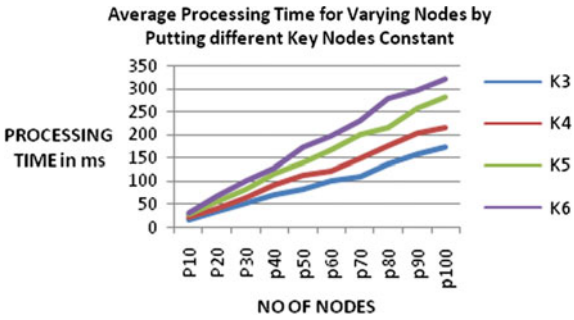

Fig. 2 Comparative total processing time for the node (range 10–100)

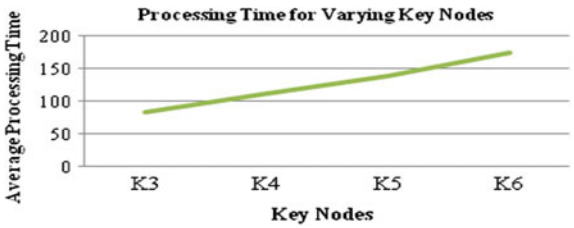

Fig. 3 Processing time for 50 nodes (key nodes 3–6)

5 Conclusion

Authentication techniques for wireless MANET are implemented using existing routing protocol or using encryption or PKI. These techniques need additional infrastructure, a centralized server in case of PKI, and huge resources to run heavy authentication algorithms. The paper has proposed an algorithm that is designed for authentication of new node who wants to join the network. The algorithm requires a minimum of 3 key nodes for the authentication process. It is found that the average processing time increases linearly as more number of nodes entered into the network and it is also found that as the number of key node increases, the processing time increases linearly. The later algorithm will be enhanced with the work of monitoring on nodes activities so that a malicious node may be excluded from the network.

References

1. Djenouri, D., Badache, N.: Survey on security issues in mobile ad hoc networks. IEEE Commun. Surv Tutor. **7**, 1–4 (2005)
2. Rubinstein, M.G., Moraes, I.M., Campista, M.E., Costa, L.H., Durate, O.C.: A survey on wireless ad hoc networks. Mobile and Wireless Communication Networks, Springer, US, pp. 1–33 (2006)
3. Bing, W., Jianmin, C., Jie, W., Mihaela, C.: A Survey on Attacks and countermeasures in Mobile Ad Hoc Networks, pp. 103–135. Wireless Network Security Signals and Communication Technology, Springer, US (2007)

4. Ma, D., Gene, T.: Security and privacy in emerging wireless networks. IEEE Wireless Commun. **17**(5), 12–21 (2010)
5. Eric, L.: Security in Wireless Ad Hoc Networks. Science Academy Transactions on Computer and Communication Networks, vol.1 (2011)
6. Pietro, R.D., Stefano, G., Nino, VV., Josep, D.-F.: Security in wireless ad-hoc networks–a survey. Comput. Commun. **51**, 1–20 (2014)
7. Nisbet, A.: The challenges in implementing security in spontaneous ad hoc networks. In: 13th Australian Information Security Management Conference, pp. 112–119 (2015)
8. Gupta, P., Bansal, P.: A Survey of Attacks and Countermeasures for Denial of Services (DoS) in Wireless Ad hoc Networks. In: 2nd International Conference on Information and Communication Technology for Competitive Strategies, ICTCS (2016)
9. Balfanz, D., Smetters, D., Stewart, P., Wong, H.C.: Talking to Strangers: Authentication in Ad-Hoc Wireless Networks. Network and Distributed System Security Symposium, NDSS (2002)
10. Andreas, H., Jon, A., Thales, N.AS.: 2-level authentication mechanism in a internet connected MANET. In: 6th Scandinavian Workshop on Wireless Ad-hoc Networks (2005)
11. Seung, Yi., Albert, F., Harris, III., Robin, K.: Quality of authentication in ad hoc networks. A Technical Report Published in College of Engineering, Illinois (2008)
12. Naveed, A., Kanhere, S.S.: Authentication and Confidentiality in Wireless Ad Hoc Networks. A book Chapter in Security in Ad Hoc and Sensor Networks. World Scientific Press (2009)