Symmetric Key Based Authentication Mechanism for Secure Communication in MANETs

Sachin Malhotra and Munesh C. Trivedi

Abstract In MANETs, secure communication is very difficult to achieve because its nature-like communication medium is open wireless which can be easily accessed by anyone who comes in the radio range of the communicating devices, nodes are physically vulnerable, less-efficient (processing power, memory) communicating devices, the absence of central authority, free from the constraint of topological structure of network, etc. In last decade, applications of MANETs are increasing rapidly. Most of the application demands the secure communication of information. In this work, symmetric key based authentication mechanism has been proposed to ensure the secure communication between the communicating parties. The proposed model secures the network from the well known and frequently occurred attacks (impersonation, modifies routing information, black hole). In this work, two levels of authentication have been used, first level for hop-to-hop authentication (MD5 algorithm has been used for authentication code generation) and second level for end-to-end authentication (SHA1 algorithm has for authentication code generation). For the simulation purpose, AODV protocol is used for checking the effectiveness of the proposed model and PDR; AE2ED and TP are used to measure the performance of the proposed, AODV and existing models in the absence and presence of the malicious nodes. NS2.35 on Ubuntu 12.04 LTS with 4 GB RAM is used for simulation. Simulation results show the advantage of proposed model over the original AODV and some related models published recently. A result showing our model implements the security scheme with less overhead.

Keywords MANETs · AODV · Attacks · Secure communication · Message authentication

S. Malhotra (✉)
Department of Information Technology, IMS, Ghaziabad, India
e-mail: sachin_malhotra123@yahoo.com

M.C. Trivedi
Department of Computer Science & Engineering, ABES Engineering College, Ghaziabad, India
e-mail: munesh.trivedi@gmail.com

Y.-C. Hu et al. (eds.), *Intelligent Communication and Computational Technologies*, Lecture Notes in Networks and Systems 19,
https://doi.org/10.1007/978-981-10-5523-2_16

1 Introduction

Suppose that we want to establish the communication connection between two floors of any organization building or between two buildings in the same campus using wireless short-range communicating electronic devices. In the organization each employee has mobile devices and some fixed devices such as printer, computer, etc. We can connect these devices using fixed wired network or by infrastructure access points, but this restricts the mob ability of the devices. Another option is used in base station based network, i.e. cellular network which allows the large communication range; but the limitation is that, these cellular networks are costly and time-consuming deploying networks. Alternatively, at last we need a network that should be fast and cheap in deployment, provide sufficient range for communication, easily scalable, support mob ability, etc., and these features are provided by only one network, i.e., mobile ad hoc network (MANET) [1, 2]. Apart from these types of applications, MANETs are also used in defense, emergency relief operations, environment monitoring, VANETs, WSNs, etc.

With the increasing number of applications, the demand for secure communication is increasing. Due to the fundament characteristics of MANET [3], secure communication is very difficult [4, 5] to achieve, because its nature-like communication medium is open wireless which can easily be accessed by anyone who are coming in the radio range of the communicating devices, nodes are physically vulnerable, less-efficient (processing power, memory) communicating devices, the absence of central authority, free from the constraint of topological structure of network, etc.

Communicating devices used in MANET have limited memory and processing power, because of this asymmetric key based security scheme is not the good solution for implementing security scheme in MANETs. With considering this limitation in mind, in this work symmetric key based authentication mechanism has proposed to ensure the secure communication between the communicating parties. The proposed model secures the network from the well-known and frequently occurred attacks (impersonation, modifies routing information, black hole). In this work, two levels of authentication have been used, first level for hop-to-hop authentication [6, 7] (MD5 algorithm has used for authentication code generation) and second level for end-to-end authentication (SHA1 algorithm has for authentication code generation). Digest_1 is the size of 128 bits generated by the MD5 algorithm and Digest_2 is the size of 160 bit generated by SHA 1 algorithm.

The remainder of this paper is organized as follows: Sect. 2 introduces related work and motivation to do this research. Section 3 describes the proposed methodology. Section 4 explains simulation result and discussion, and finally conclusion is defined in Sect. 5.

2 Related Work and Motivation

In this section, research work done in the field of secure communication in MANETs is discussed. Especially, we cover the mechanisms that have used symmetric key based security schemes. Arya K. V. and Rajput S. S. [8] have proposed the model to secure AODV routing protocol using nested MAC. In this model, the author has also used the concept of key pre-distribution (distribution of symmetric key at the time of network deployment) to overcome the drawback of methods [9] that distributes the keys at run time (when communication connection establishing between the sender and receiver). This method [8] significantly prevents the networks from many attacks (impersonation, modifies routing information, black hole). The limitation of this method is that it works efficiently when the attacker is outsider and work little bit inefficient when attacker is insider, i.e., our genuine node is compromised by the attacker.

Similar concept was used by Rajput S. S. [10] to protect MANETs against frequently occurred attacks. In this particular paper, ZRP routing protocol is used to major the performance of the proposed model. These two papers played the key role in the motivation to do the research in this field.

3 Proposed Security Mechanism

In this model, symmetric key based authentication technique is used for securing the network from various attacks. In this model, two levels of authentication are used to test the integrity of the message. The first level of authentication is used for hop-to-hop authentication and second level of authentication is used for end-to-end authentication. At first level, MD5 algorithm is used to generate 128 bits digest for checking the integrity of the message at each node of the route. SHA 1 is used to generate the 160 bits digest for checking the integrity of the message at the intended receiver of the message.

For speedup, the algorithm key table of size 15 keys (K0–K14) is stored at each node at the time of deployment. These keys are used for generating MAC (MD5) at first level that helps us to check the integrity of the message at the intermediate nodes. For generating MAC code at second level, SHA 1 uses second key generated by the random number generator. Random number generator function uses random four-digit number as seed to generate the second key.

The advantage of making two levels of authentication are to speed up the algorithm compare to Method [1], Method [2], and increase the security level. This mechanism helps us to protect our network from internal as well as external attacks.

The working model of the proposed work is given in Fig. 1. Here we are not discussing the behavior of the attacks in details. Here we are using the same behavior of the attacker as discussed in Method [1] and Method [2]. In working model as shown in Fig. 1, taking four nodes in the route one is sender node S, one

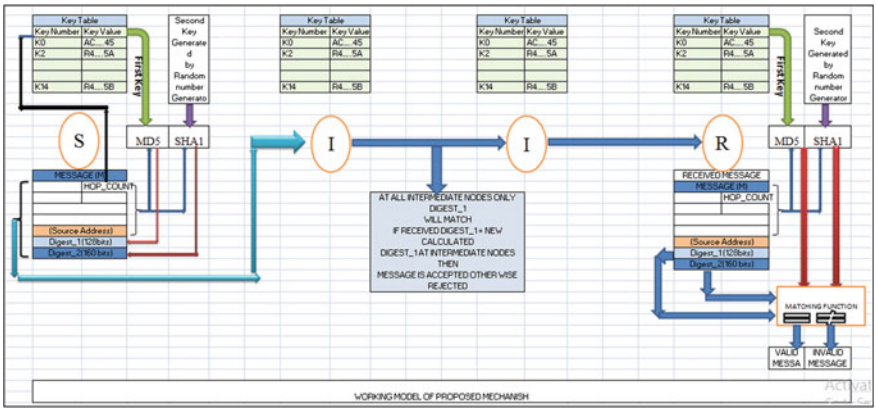

Fig. 1 Working model of proposed algorithm

is receiver node R, and two intermediate nodes I. Each node has a key table used for the authentication of the message at first level. For better understanding, whole working model is divided into three parts: Process at the Sender, Process at the receiver, and Process at the intermediate nodes.

At the sender side: Sender S first generates the message, then first key from the key table for generating the Digest_1 using MD5 is selected according to the value of hop count field in the header of the message. (First_key = Key number (Hop_count mode 15) then random number function call to generate Second_key for creating the second-level authentication code using SHA 1 algorithm then whole message (message + random 4 digit seed + Digest_1 + Digest_2) send to the next node in the route.

At the intermediate nodes, first check the integrity of the message by generating only the Digest_1 of message using the key (First_key = Key number (Hop_count mode 15) and if new Digest_1 equals to the received Digest_1, then message is treated as valid message and then again Digest_1 is created using next key in the key table and message is forwarded to the next hop in the route. If new Digest_1, does not equal the Received Digest_1 then message is treated as invalid message and message is discarded.

At the receiver side: new Digest_1 and Digest_2 is created by using First_key (First_key = Key number (Hop_count mode 15) from the key table and Second_key (generating by random number generator using same seed that has been used by the sender). If both new digest matches with received digest, then only message is received as valid message otherwise discard the invalid message. For more understanding, pseudocode for the proposed model is given in the Algorithm 1

ALGORITHM 1: ALGORITHM TO IMPLEMENT PROPOSED SECURITY MECHANISM

Abbreviations:
H_Count: Hop Count
Digist_1: 128 bits Message Authentication code generate by MD5 Algorithm
Digist_2: 160 bits Message Authentication code generate by SHA 1 Algorithm
First_Key: first key select from the key table uses by MD5
First_key = Key number (H_Count mode 15) For ex. K0, K1, --- K14
Second_Key: generating by random number generator using 4 dist seed number and
It uses by SHA 1 Algorithm
Seed: 4 digit random value
At Sender Node (S):
Step1: Generate message **M**
Step2: Select **Seed**
Step3: Select **First_Key = K0** (because **H_count** = 0 At sender) from the Key table
Step4: Generate **Second_Key**
Step5: Calculate **Digest_1** = MD5 (M, First_Key)
Step6: Calculate **Digest_2** = SHA 1 (M, Second_Key).
Step7: Send (M+Seed+Digest_1+Digest_2)

At Intermediate Nodes (I):
Step1: Receive (M+Seed+Digest_1+Digest_2)
Step2: Select **First_Key** = K(H_Count mode 15) From the Key table
Step3: Calculate **Digest_1** = MD5 (M, First_Key)
IF (**New Digest_1 = = Received Digets_1**)
THEN:
H_Count = H_Count + 1;
First_Key = K(H_Count mode 15)
Calculate **Digest_1** = MD5 (M, First_Key)
Send (M+Seed+Digest_1+Digest_2)
ELSE
Discard **M** (M is invalid);

At Receiver Node (R):
Step1: Receive (M+Seed+Digest_1+Digest_2)
Step2: Select **First_Key** = K(H_Count mode 15) From the Key table
Step3: Generate **Second_Key**
Step4: Calculate **Digest_1 = MD5** (M, First_Key)
Step5: Calculate **Digest_2 = SHA 1** (M, Second_Key).
IF (New Digest_1 = = Received Digets_1
&& New Digest_2 = = Received Digets_2)
THEN
M is valid and accepts
ELSE
Discard M (M is invalid**);**

4 Simulation and Result Analysis

To implement proposed model NS2.35 [11] has been used. Simulation parameters are given in Table 1.

In the work, proposed model is compared with original AODV, previous model was proposed by K. V. Arya and S. S. Rajput [8] (named as Method [1]) and another model was proposed by S. S. Rajput et al. [10] (named as Method [2]). Original Method [2] is proposed for the ZRP routing protocol, but in this work we have changes in this model to make it compatible with the AODV routing protocol. Performances of all the models are measured in the presence and absence of the malicious nodes in terms of AE2ED, TP, and PDR.

First we simulate, analyze, and compare the performance all four models, i.e., AODV, Method [1], Method [2], and Proposed in terms of different pause time V/s all four performance parameters (AE2ED, PDR, and Average TP). Simulation results are shown in Figs. 2, 3 and 4 shows that proposed model work better than Method [1] and Method [2] and almost similar than original AODV [12] in the absence of malicious nodes. This is because, in the proposed model at intermediate node only one digest is generating and verifying (Digest_1) while in previous model digest generated two times (used NMAC). It means proposed mechanism increases negligible over head in term of computational complexity.

Comparison of proposed model, AODV, Method [1], and Method [2] in terms of average AE2ED, PDR, Average TP with increasing number of malicious nodes (No_of_Mlcius_Nodes) shown in Figs. 5, 6 and 7. For this fixed pause

Table 1 Simulation parameters

Simulator	Ns2 (v-2.35)
Simulation time	150 s
Performance Parameters	TP (Through Put), PDR, AE2ED (Average End To End Delay)
Area size	800 m × 600 m
Transmission range	100 m
Number of nodes	10–150
Previous models	Method [1], Method [2]
Protocol	AODV
Transmission range	250 m
Maximum speed	0–20 m/s
Application traffic	CBR
Packet size	512 bytes
Traffic rate	4 packet/s
Node mobility model	Random Way-Point Model
Pause time	10, 20, 60, 100–140 s
Mac method	802.15.4

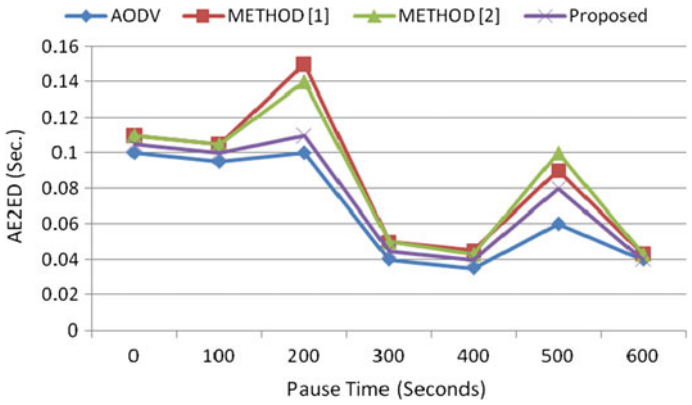

Fig. 2 Pause_Time versus AE2E Delay

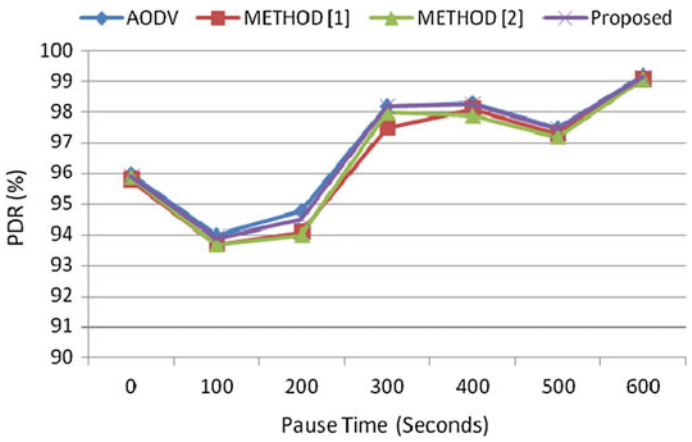

Fig. 3 Pause_Time versus PDR

time = 300 s and number of connections = 10 have been used. Results show that proposed model performing outstanding as comparing to the other three models in the presence of malicious nodes. Out of all malicious nodes in each simulation, 50% nodes are taken as inside attackers and remaining 50% as outside attacker. Simulation results also show that our model perform better in the presence of inside attacker; it means our model significantly overcomes the drawback of Method [1] and Method [2].

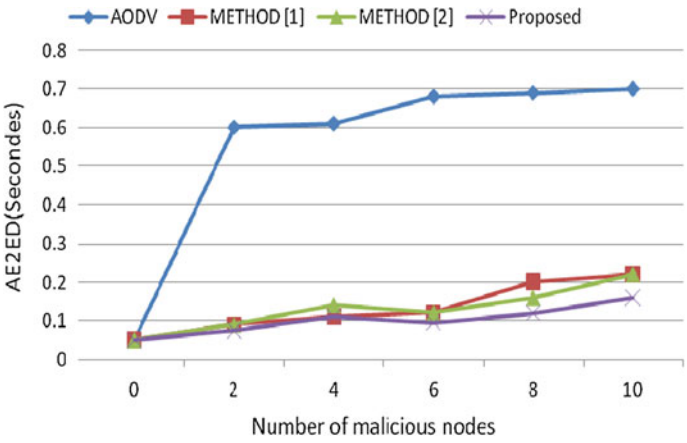

Fig. 4 Pause_Time versus Average_TP

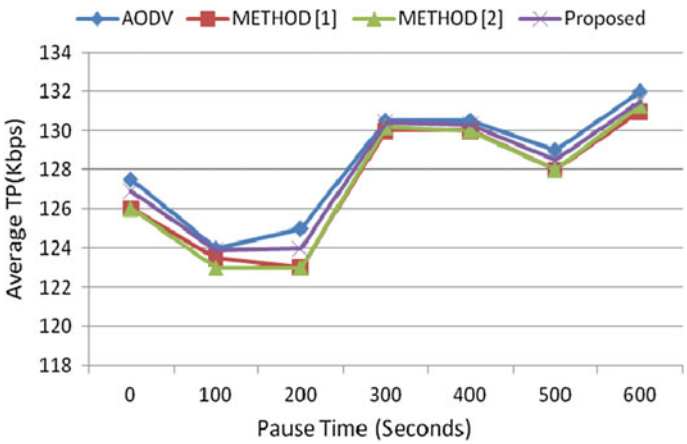

Fig. 5 AE2E Delay versus No_of_Mlcius_Nodes

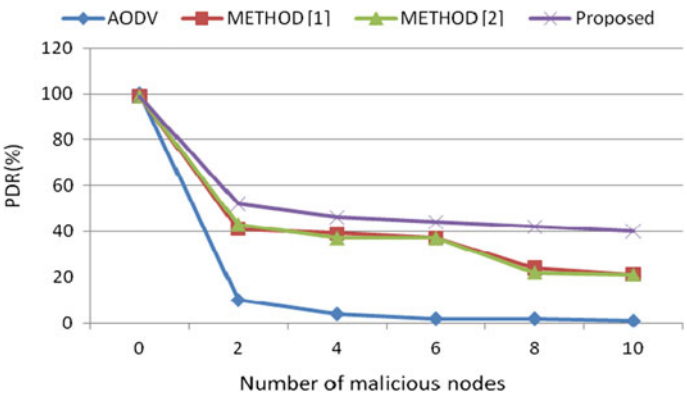

Fig. 6 PDR versus No_of_Mlcius_Nodes

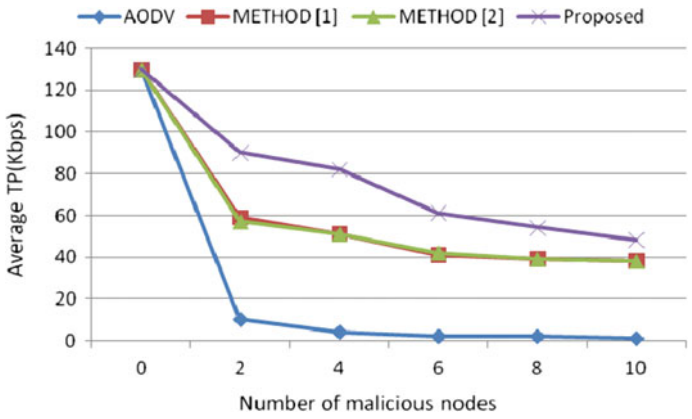

Fig. 7 Average_TP versus No_of_Mlcius_Nodes

5 Conclusion

In this paper, symmetric key based authentication mechanism has been proposed to secure the AODV against various attacks (impersonation, modifies routing information, black hole). Simulation results show that proposed model work better than Method [1] and Method [2] and almost similar than original AODV in the absence of malicious nodes. It means proposed mechanism increases negligibly over head in terms of computational complexity. Results also show that proposed model perform in an outstanding way compared to the other three models in the presence of malicious nodes. Out of all malicious nodes in each simulation, 50% nodes are taken as inside attackers, and remaining 50% as outside attacker. Simulation results also show that our model performs better in the presence of inside attacker; it means our model significantly overcomes the drawback of Method [1] and Method [2].

References

1. N. Sharma, A Gupta, SS Rajput and V. Yadav, " Congestion Control Technique in MANET: A Survey" 2nd IEEE International Conference on CICT, pp. 280–282, Feb. 2016.
2. S. S. Rajput, V. Kumar and S. K. Paul, "Comparative Analysis of Random Early Detection (RED) and Virtual Output Queue (VOQ) in Differential Service Networks" IEEE International Conference on SPIN, pp. 281–285, Feb 2014.
3. S. S. Rajput, V. Kumar and K. Dubey, "Comparative Analysis of AODV and AODV-DOR routing protocol in MANET" International Journal of Computer Application, vol. 63, no. 22, pp. 19–24, Feb 2013.
4. D. Djenouri et al. "A survey of security issues in mobile ad hoc networks" IEEE Communications Surveys & Tutorials. Fourth Quarter 2005.
5. M. Charvalho, "Security in Mobile Ad hoc Networks" Published by the IEEE Computer S ociety, pp:72–75, 2008.

6. William Stalling, Cryptography and Network Security, 4th Ed. Pearson Education, India, 2006.
7. B. A. Forouzan, Cryptography and Network Security, 2nd Ed., Tata McGraw-Hill Higher Education, India, 2008.
8. K. V. Arya and S. S. Rajput, "Securing AODV routing protocol in MANET using NMAC with HBKS Technique," IEEE International Conference on SPIN, pp. 281–285, Feb 2014.
9. P. Sachan and P. M. Khilar, "Securing AODV routing protocol in MANET based on cryptographic authentication mechanism," International Journal of Network Security and Its Applications (IJNSA), vol. 3, no. 5, 2011.
10. S. S. Rajput and M. C. Trivedi, "Securing ZRP routing protocol in MANET using Authentication Technique," IEEE International Conference on CICN, pp. 872–877, Nov. 2014.
11. E. H. T. Issariyakul, "Introduction to Network Simulator NS2," Springer Science and Business Media, NY, USA, 2009.
12. C. Perkins, E. Beldingroyer, and S. Das, "AODV RFC 3561," Internet Engineering Task Force (IETF), 2003. Available at http://datatracker.ietf.org/doc/rfc3561/.