International Journal of Innovation and Applied Studies
ISSN 2028-9324 Vol. 5 No. 3 Mar. 2014, pp. 294-300

http://www.issr-journals.org/ijias/

Achieving MANETs Security by Exchanging Path Oriented Keys and Priority Based Secured Route Discovery

N. Chandrakant

Department of Computer Science and Engineering,
UVCE, Bangalore University,
Bangalore, Karnataka, India

ABSTRACT: In this work, two scenarios are considered, scenario-1 is key based communication and scenario-2 is priority based routing and communication. In scenario-1, MANET works on generated keys called KEY1 and KEY2 to establish communication between nodes. Here source node will have to generate and store a key called KEY2 and destination node will have to generate and store a key called KEY1. When source node initiates communication with destination-node, source node will send a request-packet to destination via shortest/less- cost path (PATH1) without any key mentioning in the packet. Now destination node will send the requested packet and KEY1 to source node via different path other than PATH1 (path of received packet). Source will send KEY2 to destination again through the same path (PATH2). In scenario-2, communication of each node is based on the neighbour node's priority, here, priority-1 being the highest, hence it is highly recommended for communication and priority three is being the lowest and it is rarely recommended for the communication. Nodes in the network classified into 3 types, unknown node, neighbor's known node, non-neighbors known node. Priority of nodes can be evaluated based on the security measures, energy level and other parameters of the node. It can also consider Trust Value (TV) of each node based on the duration spent in active efficient communication. With help of this strategy, we can achieve highly secured route discovery, which will help network to have smooth communication among its nodes.

KEYWORDS: Generated Key, Alternative Path, AODV, DSR, DSDV, Priority.

1 INTRODUCTION

Mobile Ad-Hoc Networks (MANET) is an infrastructureless network with limited provisioning of security, size, battery life, speed etc. Hence MANETs are more exposed to hackers including secret key breaking [1]. The routing process can be disrupted by internal or external attackers. Security threatening can affect even energy of the nodes; hence we need to achieve security goals as much as we can. These goals can include, confidentially, authentication, integrity, non-repudiation, availability, access Control etc. Since MANETs have a nature of ad hoc network formation in which nodes can join and leave easily with dynamics requests without a constant path of routing. These attacks are classified based on layers of MANETs which are mostly affected, application layer can have problems due to malicious code and repudiation; transport layer can have problems when session is hijacked or flooding the packets; attacks of network layer includes Sybil, worm/black/grey hole, link spoofing/withholding etc. ; data Link/MAC layer can be affected due to malicious behaviour of nodes, selfish behaviour, active/passive attacks, etc.; finally, physical layer can includes attacks such as interference, traffic jamming, eavesdropping etc. Due to the nature of MANETs, the design, development and implementation of secure routing is challenging work for researchers in an open and distributed communication environment. Hence, this work presents a novel approach to contribute the security goals where keys of source and destination nodes are shared through an alternative path such that nobody can misuse these keys.

The security requirements of MANETs include; availability, integrity, confidentiality, authentication and non-repudiation, because it is more susceptible to security attacks than fixed networks due to their inherent characteristics.

Corresponding Author: N. Chandrakant (chandrakant.naikodi@yahoo.in)

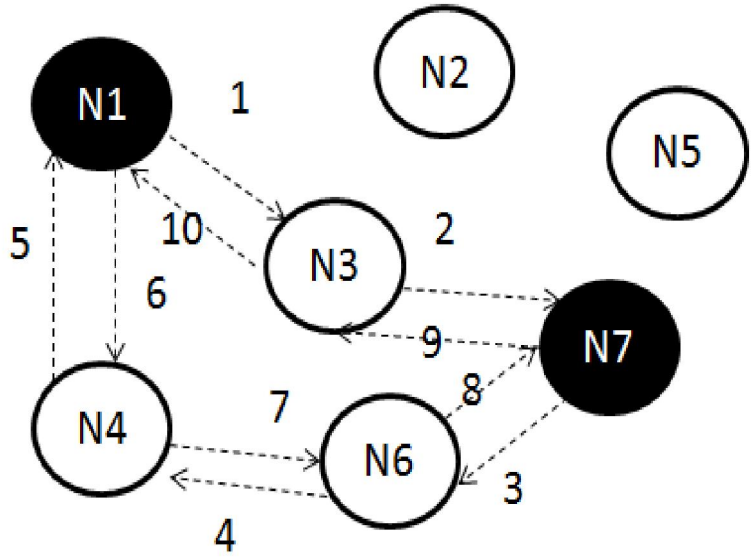
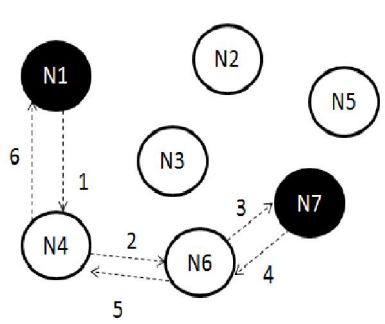


Fig. 1. Sample Nodes Communication for Scenario-1



For Steps:1,2,3

RReq
ID:1001 Src:N1 Dst:N7 LifeSpan:3

For Steps:4,5,6

RRep
ID:1001 Src:N1 Dst:N7

Table for N1 :

Node Id	Node Name	Old Priority(1-3)	Current Priority(1-3)
N1	1000001	-	-
N2	1000002	-	2
N3	1000003	3	3
N4	1000004	1	1
:	:	:	:

Fig. 2. Sample Nodes Communication for Scenario-2

The universal network goals of security like privacy, data accessibility, integrity, authenticity and non-repudiation are little hard to achieve in wireless network like MANET,WSN etc, this can be due to its open environment where all nodes co-operate in forwarding the packets in the network like hop-by-hop. Comparing to wired networks, wireless networks has more challenges in detecting fraud nodes or malicious nodes. Hence, allowing for overall research and its upcoming security challenges, it is fairly difficult to design a hundred percent secure protocol for WSN/MANET.

The organization of work goes like this, section 2 details about recent research in security of MANET's communication. Detailed design of two scenarios and its implementation with results has been explained in section 3. Finally, section 4 concludes the work and gives an outlook to further research.

2 LITERATURE SURVEY

This work has been improved and integrated two previous works [2] and [3]. Preeti and Sumitha [1] has analysed the MANETs in terms of security issues that are currently faced by the network including Bio-inspired Algorithms. BFOA (Bacterial foraging optimization algorithm) algorithm simulates behaviour of bacteria that can be effectively applied in various fields; hence this can be applied to secure the MANETs too. Reference [4] highlights about security architecture design and analysed features, insecurity factors and security threats of MANETs. The author used OSI hierarchy model as a reference model to design security architecture. The investigation on association between each layer of the architecture and that of OSI was also provided, which offers framework for planning and designing safe and consistent MANET. Reference [5] presents a concept of Dezert-Smarandache theory application for enhancing security in tactical MANET. The strategic MANET, due to its requirement, requires collection and processing of information from different sources of varied security and confidence metrics. The authors identified the needs for building a node's situational awareness and recognize data sources used for calculations of trust metrics. They provided some examples of connected works and presented their own conception of Dezert-Smarandache theory applicability for trust assessment in mobile hostile environment. Reference [6] presents a novel security mechanism to enhance security and performance of AODV (Adhoc On-demand Distance Vector) routing protocol under the attack for MANET. A robust key-management system with energy efficient is required to meet the security mechanisms of AVODV. Therefore, authors have proposed a novel security mechanism where digital signature and hash chain are integrated to protect the AODV routing protocol.

Reference [7] presents the major components of the security level of MANETs. Security issues of Data Query Processing and Location Monitoring. The security level assessment architecture, security level categorization and in applications is also presented.

Reference [8] highlighted ad-hoc network challenges and its affect on operations. Described about primary limitation of the MANETs like restricted resource capability that is, bandwidth, power back up and computational capacity etc. This stuff also affects the existing security schemes for wireless networks which makes them much more susceptible to security attacks.

Shakshuki et al. [9] has examined the study of self configuring nodes in the MANETs. Since MANET has the open communication medium and broad distribution of nodes make its more vulnerable to malevolent attackers. Hence, author recommended developing proficient intrusion-detection mechanisms to safeguard MANET from attacks with the developments of the technology and cut in hardware costs. To regulate such kind of movement, they muscularly believed that it is essential to address its potential security issues.

Tamilarasi, et al. [10] has analysed the energy desires of various cryptographic primitives with the purpose of using this data as a base for devising energy efficient security protocols also they have measured delay, packet delivery ratio and routing overhead to evaluate best security algorithm.

Reference [11] has proposed a conviction method for ad hoc network via three steps, they are honoring, calculating, and using the trust as a foundation to set up keys between the nodes in adhoc network, and make use of this belief as a measurement for setting up secure distributed control in ad hoc network. Mutual trust has been used to make decisions on establishing connection between group and/or pair wise keys.

Reference [12] highlighted MANET's challenges and its affect on operations. Described about primary limitation of the MANETs like limited resource capability that is, bandwidth, power back up and computational capacity etc. These things also affect the existing security schemes for wireless networks which makes them much more vulnerable to security [13] attacks.

Prajeet and co-authors [14] has proposed a mechanism which eliminates the need for a centralized trusted authority which is not practical in MANETs due to their self organizing nature. This mechanism defends the MANET through a self organized, fully distributed and localized procedure. The extra certificate publishing occurs only for a small amount of duration during which almost all nodes in the network get certified by their neighbors. After a period of time each node has a directory of certificates and hence the routing load sustained in this process is reasonable with a good network performance in terms of security as compare with attack case. The proposed mechanism can also be useful for securing the network from other routing attacks by altering the security parameters in harmony with the nature of the attacks.

Wireless devices in MANET communicates directly with each other when they are both within the same signal range else they rely on their neighbors to resend the messages. Shakshuki et al. [15] has examined the study of self-configuring nodes in the MANETs. Since MANET has the open communication medium and broad distribution of nodes make its more susceptible to malevolent attackers. Hence, author urged to develop proficient intrusion-detection mechanisms to guard MANET from attacks with the developments of the technology and cut in hardware costs. To adjust such kind of trend, they muscularly believed that it is essential to address its potential security issues. Finally, they anticipated and implemented a new intrusion-detection system named Enhanced Adaptive Acknowledgment (EAACK) particularly designed for MANETs. Compared to modern approaches, EAACK demonstrates higher malicious-behaviour-detection rates in definite condition while does not greatly influence the network performances.

3 DETAIL DESIGN

In this section, two abstracted scenarios are explained along with performance results. Below scenarios are extended from [16] and [17].

3.1 SCENARIO-1: KEY EXCHANGE METHOD

The overall communication sample is shown in Fig 1. In the figure, N1(src) wants to send RReq packet to N7(dst). N1 sends RReq packet to N3, and N3 sends same to N7. Here N7 does not reply back to N3 or does not reply back to the same node which has sent a RReq. N7 will choose a different/alternative path to validate the request of N3. Now N7 sends a RReq packet with secret KEY1 to N1 via N6 and N4, then N1 will reply back((RRep) to N7 with its own secret key called KEY2. Now N7 will validate and cross check the previous request and proceeds communication with N3 (previous path) with KEY2 being part of every packet and this is understood by N1 only. KEY1 and KEY2 needs to be stored in N1 to decrepit the packets of N7 for next communication. KEY1 will expire after communication session ends between nodes. KEY1 and KEY2 will be stored in N1 and N7 until session of communication ends, then this key will expiry. KEY1 and KEY2 should be used for particular session to decrepit each packet.

The basic algorithm of above proposal is specified in Algorithm 1 which describes major steps involved in the communication establishment and progress.

The simulation results are drawn in a graph for DSR, AODV and proposed algorithm is shown in Figure 3. The simulation experiment is implemented in JAVA with 100 nodes as network size. The packet End-to- End delay is the average time that a packet obtains to traverse the MANET. The delay includes the time from the generation of the packet in the source or sender up to its reception at the application layer of destination including all the delays in the network such as transmission time, buffer queues and delays induced by routing activities and MAC control exchanges. Hence, End-to- End delay is depends upon how well a routing protocol adapts to the variety of constraints in the network and represents the consistency of the routing protocol. As shown in figure, DSR shows better performance than AODV and proposed algorithm because AODV and proposed algorithm needs more time in route discovery where as DSR works on a static path routing , hence our algorithm it produces slightly more End-to-End delay than DSR but almost same as AODV. Hence, considering security perspective and above study on End- to-End delay, the proposed algorithm has higher consistency w.r.t secured communication than AODV and DSR.

3.2 SCENARIO-2: PRIORITY BASED ROUTING

The proposed algorithm has been simulated in Java and the overall working scenario is shown in Fig 2. In this figure, N1 (Source Node) wants to send an RReq packet to N7 (Destination Node), N2, N3 and N4 are neighbors of N1, from N1 to N7, there are 3 paths existed via N2, N3, and N4. Here, N1 will choose N4 for immediate communication as N2 and N3 has lower priority value compare to N4. After establishing a path, N7 sends RRep packet to N1. Hence, communication and packets are more secured through such enforcement.

In this approach we used 3 terms as follows,

Neighbors known node:

These nodes are immediate neighbors and are listed in the table along with their priority values. All neighbors need not have priority one. These nodes can be suffered from battery/energy, performance and other parameters; hence priority can vary from time to time.

Non-neighbors known node:

As its name says, these nodes are belonging to neighbors of neighbors. Here too, all neighbors need not have priority one.

Unknown node:

This node is no where listed in the table of neighbors; hence it has last priority (3). These nodes can have more battery/energy and can perform better in terms of speed.

There are few drawbacks of this approach, which includes, route could be longer than non-trusted or less priority node's path and network life time can be affected. If you need high security, we need to compromise few parameters like performance, energy etc.

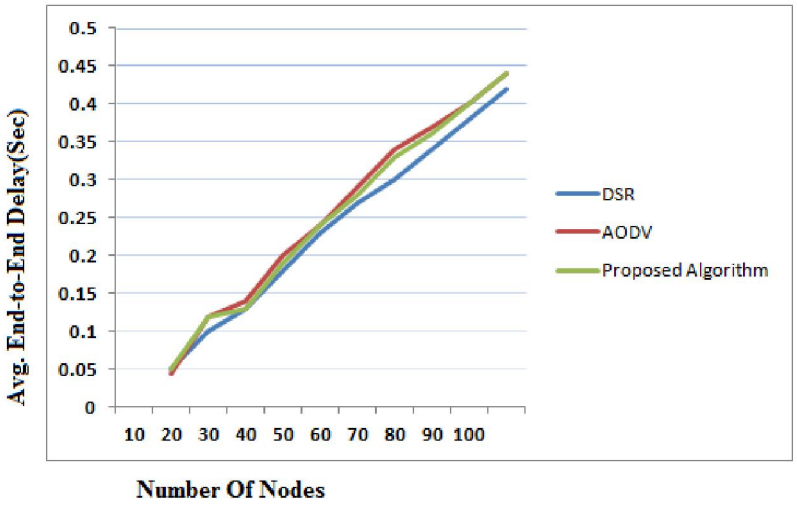


Fig. 3. End-to-end delay of DSR, AODV and Proposed Algorithm for Scenario-1

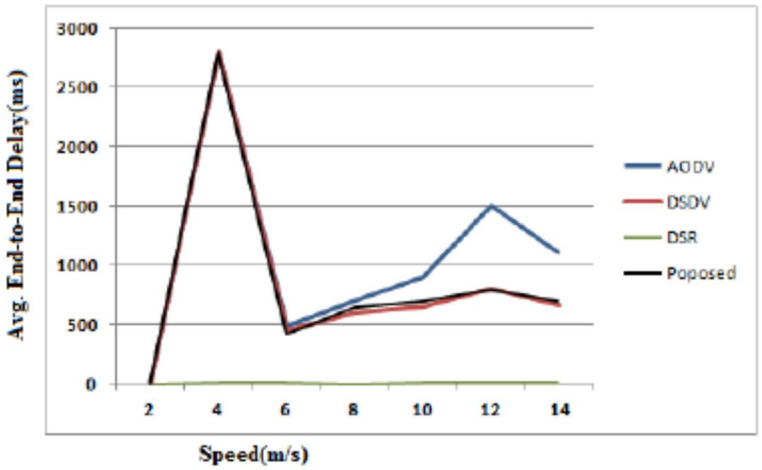


Fig. 4. End-to-End Delay V/S Mobility Response in MANET for Scenario-1

Important scenarios where algorithm needs to consider maximum security while nodes are above to initiate the communication or if communication is already progressing. Such scenarios are listed below:

1. How to do initial deployment of network?

When first time network is deployed, all nodes will have equal priority for each neighbour, here, if a node wants to communicate with other node, then it can choose any nodes for that matter or you can assign a priority considering resource constraints.

2. What happens when higher priority neighbour disappeared/dead/battery exhausted/left network?

This is one of the scenarios where communication link can be broken. If higher priority node is not available/disappeared, then next available priority node will be chosen for communication.

3. What happens when an unknown node enters into network?

Here we need to consider malicious and non- malicious nodes entry into network and needs to scrutinize the nodes based on validation.

4. What happens if legitimate Neighbour got infected with unusual behaviour like virus infected etc?

Here accessing node/genuine node needs to broadcast about malicious node participation to all other nodes and their tables can be updated for this particular node.

The figure 4 shows that DSR protocol has the lowest delay as compared to other protocols. AODV and DSDV have more or less same delay. The proposed algorithm and AODV has moderately more delay than DSR and DSDV, this is due to the source routing impression of DSR . Because DSR has all precalculated paths, that will help to have better performance than others. The proposed algorithm and AODV would have to send/calculate a specific request/path for that destination [18]. Before a path confirmation, the packets have to wait in a buffer until a valid route is found; hence this will take some time which increase the average delay as mobility rises.

Algorithm 1 $main()$

Require: Initialize $path1 \leftarrow null, path2 \leftarrow null, src \leftarrow null, dst \leftarrow null, n \leftarrow numberOfNodes, i \leftarrow 0, j \leftarrow 0, nodes[] \leftarrow listOfNodes, key1 \leftarrow 0, key2 \leftarrow 0$

```
1:  while i++ <= n do
2:    if nodes[i] ==' src' then
3:      key2 = generateRandomKey(nodes[i])
4:      while j++ <= n do
5:        if nodes[j] ==' dst' then
6:          key1 = generateRandomKey(nodes[j])
7:        end if
8:      end while
9:      src = nodes[i], dst = nodes[j]
10:     path1 = generateShortestPath(src,dst)
11:     path2 = generateRandomPath(src,dst)
12:     acknowledgement1=initializeCommunication(src,ds
        path1);
13:     acknowledgement2=initializeCommunication(dst,sr
        path2);
14:     acknowledgement3=initializeCommunication(src,ds
        path2);
15:     if acknowledgement2 contains key = key1 )
        then
16:       if acknowledgement3 contains key =
          key2 ) then
17:         proceedCommunication(src,dst,path1)
18:       end if
19:     end if
20:   else
21:     exit
22:   end if
23: end while
```

4 CONCLUSION

Based on the scenarios conclusion, Scenario-1 has proposed a novel approach where generated keys are used to authenticate each other by exchanging the keys via unusual paths (other than shortest path). Here both side communications should have keys of respective parties. I.e. source packet should have KEY1 and destination packet should have KEY2 and

these keys are compared for authentication purpose and evaluated accordingly. KEY1 and KEY2 keys are shared before the communication establishment and it will expire after each session exit. Hence, considering overall performance of simulation and strategy, the proposed idea is one the best method for secured communication. This work can be enhanced to support multi-key and multi-path routing so that security is much stronger.

Scenario-2 tries to propose a robust algorithm which protects nodes communication in a MANET. For communication with/via a neighbour is based on the neighbors node's priority, here, priority-1 being the highest hence it is highly recommended for communication and priority three is being the lowest and it is rarely recommended for communication. Priority of nodes can be evaluated based on the Trust Value, resource crunch, security measures and other parameters of the node. Trust Value (TV) of each node can be based on the duration spent in active efficient communication, history, etc. This strategy helps to choose a highly secured route which will help network to have a better communication among its nodes.

REFERENCES

[1] P. Gulia and S. Sihag, "Review and analysis of the security issues in MANET", International Journal of Computer Applications, 75(8), 23–26, August 2013.

[2] Chandrakant N, "Priority based secured route discovery in MANETs", In International Journal of Computer Science and Information Technology Research Excellence (IJCSITRE), Vol. 3, Issue 5, ISSN NO. 2250-2734, EISSN NO. 2250-2742, pages 17–20, 2013.

[3] Anil Choudhary, Dr O P Roy and Dr T Tuithung, "Performance analysis of routing protocols for mobile ad-hoc networks", IJIET, Vol-2, Issue-2, ISSN: 2319-1058, pages 327–336, Apr 2013.

[4] L. Shi-Chang, Y. Hao-Lan, and Z. Qing-Sheng, "Research on MANET security architecture design", International Conference on Signal Acquisition and Processing- ICSAP '10, pages 90–93, 2010.

[5] J. Glowacka and M. Amanowicz, "Application of dezertsmarandache theory for tactical MANET security enhancement", International Conference on Communications and Information Systems Conference (MCC), pages 1–6, 2012.

[6] S. Soni and S. Nayak, "Enhancing security features amp; performance of AODV protocol under attack for MANET", International Conference on Intelligent Systems and Signal Processing (ISSP), pages 325–328, 2013.

[7] M. Qayyum, P. Subhash, and M. Husamuddin, "Security issues of data query processing and location monitoring in MANETs", International Conference on Communication, Information Computing Technology (ICCICT), pages 1–5, 2012.

[8] S. J. Sudhir Agrawal and S. Sharma, "A survey of routing attacks and security measures in mobile ad-hoc net- works", JOURNAL OF COMPUTING, VOLUME 3, ISSUE 1, ISSN 2151-9617, pages 41–48, 2011.

[9] Shakshuki, E.M. and Nan Kang and Sheltami, T.R. Eaack, "A secure intrusion-detection system for MANETs", Volume 60, pages 1089–1098, 2013.

[10] Tamilarasi, M. and Sundararajan, T. V P, "Secure enhancement scheme for detecting selfish nodes in MANET", International Conference on Computing, Communication and Applications (IC- CCA), pages 1–5, 2012.

[11] R. Ferdous, V. Muthukkumarasamy, and A. Sattar, "Trust formalization in mobile ad-hoc networks", 24th International Conference on Advanced Information Networking and Applications Workshops (WAINA), pages 351–356, 2010.

[12] S. J. Sudhir Agrawal and S. Sharma, "A survey of routing attacks and security measures in mobile ad-hoc net- works", JOURNAL OF COMPUTING, VOLUME 3, ISSUE 1, ISSN 2151-9617, pages 41–48, 2011.

[13] Javad Pashaei Barbin, Mohammad Masdari, "Enhancing name resolution security in mobile ad hoc networks", International Journal of Advanced Science and Technology, pages 41–50, Jan 2013.

[14] N. S. Prajeet Sharma and R. Singh, "A secure intrusion detection system against DDOS attack in wireless mobile ad-hoc network", International Journal of Computer Applications (0975 8887), Volume 41 No.21, pages 16– 21, 2012.

[15] Shakshuki, E.M. and Nan Kang and Sheltami, T.R.Eaack, "A secure intrusion-detection system for MANETs", Volume 60, pages 1089–1098, 2013.

[16] Chandrakant N, "Exchanging path oriented n-generated keys via alternative path for secured communication in MANETs", International Journal of Inventive Engineering and Sciences (IJIES), Volume-1, Issue-11, ISSN: 23199598, pages 44–46, 2013.

[17] Chandrakant N, "Achieving MANETs security by exchanging path oriented single or n-generated keys via secondary path", International Journal of Science and Technology (IJST), Volume 3 Issue 2, ISSN (online): 2250-141X, pages 23–29, 2013.

[18] Sunil Taneja, Ashwani Kush, and Amandeep Makkar, "End to end delay analysis of prominent on-demand routing protocols", International Journal of Computer Science and Technology, Vol-2,Issue-1, ISSN:0976-8491, pages 42–46, March 2011.