ISSN (online): 2250-141X
Vol. 3 Issue 2, October 2013

DETECTING MALICIOUS NODES USING KEY SHARING TECHNIQUES THROUGH ALTERNATIVE PATH AND KEY GENERATION FOR SECURED COMMUNICATION IN MANETS

Chandrakant N
Bangalore, India

Abstract— **In this network, after nodes deployment, each node will have or calculate Trust Value (TV) for all its neighbors based on its performance, efficiency, QOS and other parameters. If anybody wants to communicate with any other node, then source node must ask its neighbours to choose possible PATH2 and not to select certain path or not to select most expected path i.e. PATH1 which is low cost/shortest path, then source node will send a secret key or secret path route key(summation/manipulation of all nodes in the path) to the seeking node, then seeker node will hold/save the key for fixed amount of time. This process happens for all nodes of a particular path which is going to involve in the communication. After this process, source node will ask key form all nodes of shortest/low-cost path called PATH1 and verify the same key with the one which has sent earlier to those nodes. In this way, we can eliminate the malicious nodes as these nodes are unable to send the key which is asked by any other nodes. Hence, it ensures secured communication among genuine nodes.**

Keywords: MANET, Malicious, Alternative Path, Inter- mediate Key

I. 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 [4]. 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 open and distributed communication environments.

The organization of paper goes like this, section 2 details about recent research in security of MANETs communication. Detailed design and its implementation with results have been explained in section 3. Finally, section 4 concludes the paper and gives an out- look to further research.

ISSN (online): 2250-141X
Vol. 3 Issue 2, October 2013

II. Literature Survey

This paper is the enhancement of paper [1] and paper [2]. The article [3] presents a concept of DezertSmarandache theory application for enhancing security in tactical MANET. The strategic MANET, due to its requirement, requires collection and processing of in- formation 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 DezertSmarandache theory applicability for trust assessment in mobile hostile environment. Preeti and Sumitha [4] 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. Paper [8] 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.

Algorithm 1 $main()$

Require: Initialize $path1 \leftarrow null, path2 \leftarrow null, src \leftarrow null, dst \leftarrow null, n \leftarrow numberOfNodes, i \leftarrow 0, j \leftarrow 0, nodes[] \leftarrow listOfNodes, IKn-2 \leftarrow 0, key1 \leftarrow 0, key2 \leftarrow 0, TVs \leftarrow 0, TVd \leftarrow 0, minTV \leftarrow 90$

```
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:        IKn-2 = generateRandomKey(nodes[j])
9:      end while
10:     src = nodes[i], dst = nodes[j]
11:     TVs = TVOfNode(nodes[i]), TVd = TVOfN-
        ode(nodes[j])
12:     path1 = generateShortestPath(src,dst), path2
        = generateRandomPath(src,dst), acknowl-
        edgement1=initializeCommunication(src,dst,
        path1),acknowledgement2=
        initializeCommunication(dst,src, path2);
13:     acknowledgement3=initializeCommunication(src,dst
        path2);
14:     if ( acknowledgement1 contains key =
        IKn-2 )AND ( acknowledgement2
        contains key = key1 ) AND (
        acknowledgement3 contains key = key2 )
        AND(TVs ≥ minTV AND TVd ≥ minTV
        ) then
15:       proceedCommunication(src,dst,path1)
16:     end if
17:   else
18:     exit
19:   end if
20: end while
```

Shakshuki et al. [7] 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.

Paper [9] presents a novel security mechanism to enhance security and performance of AODV (Adhoc On-demand Distance Vector) routing protocol under the attack for MANET. The security mechanisms that are available in AVODV can consume more processing power and required

ISSN (online): 2250-141X
Vol. 3 Issue 2, October 2013

complex key-management system. Hence, they presented a novel security mechanism that integrates digital signature and hash chain to defend the AODV routing protocol that is capable of defending it- self against both malicious and unauthenticated nodes with marginal performance variation.

In paper [10], 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.

Tamilarasi, et al. [11] has analysed the energy de- sires of various cryptographic primitives with the purpose of using this data as a base for devising energy- efficient security protocols also they have measured de- lay, packet delivery ratio and routing overhead to evaluate best security algorithm.

Paper [6] 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.

Dynamic and link-state routing algorithms do not give a schemes to guard data or sensitive outing information since any centralized entity could lead to considerable vulnerability in MANETs[5].

III. Detail Design

The overall Architecture 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 with its own generated key called IK1(IKn-2,n>3).

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 N1/N3. Now N7 sends a RReq packet with secret KEY1 and IK1 to N1 via N6 and N4, now 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,IK1 being part of every packet which is understood by N1 only. KEY1,KEY2 and IK1 needs to be stored in N1 to decrepit the packets of N7 for next communication. KEY1,KEY2 and IK1 will expire after communication session ends between nodes. KEY1,KEY2 and IK1 will be stored in N1,N7 until session of communication ends, then this key will expiry. KEY1, KEY2 and IK1 should be used for particular session to decrepit each packet. If PATH2 does not exist in the network, then PATH1 will be used in such case.

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

The simulation results are shown in Figure 2. The simulation experiment is implemented in JAVA with 100 nodes as network size.

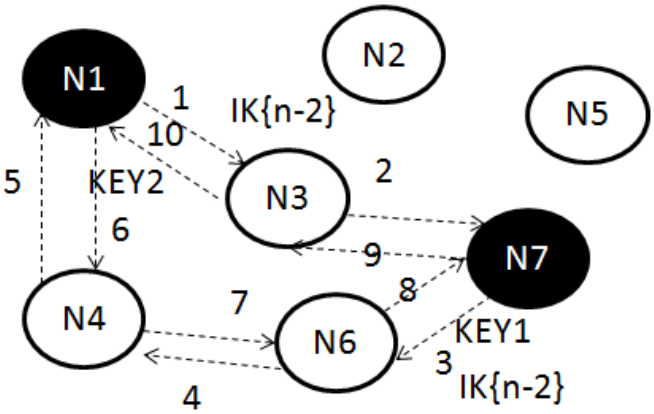

Figure 1. Sample Nodes Communication

ISSN (online): 2250-141X
Vol. 3 Issue 2, October 2013

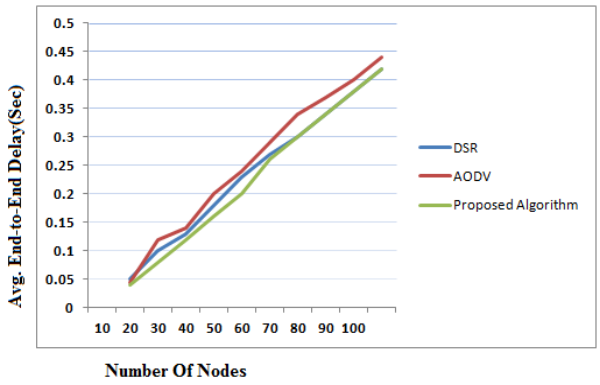

Figure 2. End-to-End Delay of DSR, AODV and Proposed Algorithm

The packet End-to-End de- lay is the average time that a message obtains to traverse the MANET. The delay includes the time from the generation of the message 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, similarly proposed algorithm too shows better performance than AODV, and hence the proposed algorithm produces End-to-End delay almost equal to DSR. Hence, considering security perspective and above study on End-to-End delay, the proposed algorithm has high consistency w.r.t secured communication than AODV and DSR.

IV. Conclusion

A novel approach has been proposed in this paper, nodes authenticate based on Trust Value, where source node will ask a key form all nodes of shortest/low-cost path called PATH1 and verify the same key with the one which has sent earlier to those nodes. This strategy can eliminate the malicious nodes as these nodes are un- able to send the key which is asked by any other nodes. Hence, it ensures that secured communication can hap- pen between genuine nodes only.

References

[1] Chandrakant N. Exchanging generated keys via alternative path for secured communication in MANETs. In International Journal of Computer Science and Information Technology Research Excellence (IJCSITRE), Vol.3, Issue 5,ISSN NO. 22502734, EISSN NO. 22502742, 2013.

[2] Chandrakant N. Exchanging path oriented n-generated keys via alternative path for secured communication in MANETs. In International Journal of Inventive Engineering and Sciences (IJIES), Volume1, Issue11, Oct. 2013, ISSN: 23199598, pages 44–46, 2013.

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

[4] P. Gulia and S. Sihag. Article: Review and analysis of the security issues in MANET. International Journal of Computer Applications, 75(8):23–26, August 2013. Published by Foundation of Computer Science, New York, USA.

[5] Nikola Milanovic Miroslaw Malek, Anthony Davidson, Veljko Milutinovic. Routing and security in mobile ad hoc networks. In Published by the IEEE Computer Society, pages 61–65, 2004.

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

[7] Shakshuki, E.M. and Nan Kang and Sheltami, T.R. Eaack:a secure intrusion-detection system for MANETs. volume 60, pages 1089–1098, 2013.

[8] L. Shi-Chang, Y. Hao-Lan, and Z. Qing-Sheng. Research on MANET security architecture

ISSN (online): 2250-141X
Vol. 3 Issue 2, October 2013

design. In Signal Acquisition and Processing, 2010. ICSAP '10. International Conference on, pages 90–93, 2010.

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

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

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