Exchanging Path Oriented N-Generated Keys Via Alternative Path for Secured Communication in MANETs

Chandrakant N

Abstract— In this paper, communication in a MANET works on key sharing called KEY1 and KEY2 to establish link between nodes. Here source node will generate and stores KEY2 and destination node will generate and stores KEY1. When source node initiates communication for destination, source node will send a request packet to destination via shortest/less cost path (PATH1). Here PATH1 can have many nodes and each node will generate a secret key whenever it receives a packet for first time for a particular session. Now that packet should take this key and move ahead to next node, similarly, next node too generates a secret key and appends to this packet, this task will be continued until packet reaches its destination, these all intermediate keys (IK) are merged (like applying arithmetic or logical operation) to form a unique key in the destination called as IKn2 where n>2 i.e excluding source node and destination node. Both side communications should have respective node's keys. i.e source packet should have KEY1,IKn2 and destination packet should have KEY2,IKn2. KEY1, KEY2 and IKn2 will expire after each session ends. So keys are shared before communication establishment.

Keywords: MANET, IKn2, Alternative Path, Intermediate Key

I. INTRODUCTION

Mobile AdHoc Networks (MANET) is an autonomous collection of mobile nodes that communicate over bandwidth/energy/memory/processor constrained wireless links. This nature makes MANETs more exposed to hackers including secret key cracking [2]. 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, nonrepudiation, availability, access Control etc. Hackers can attack the MANET to delete packets, messages, manipulate data and make erroneous messages, or impersonate a node, which violates authentication, availability, integrity, and nonrepudiation. The attacked nodes also can begin attacks from within a network. Dynamic and linkstate 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[3].

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.

Nodes in adhoc network can join and leave easily with dynamics requests without a constant path of routing, this nature makes challenging in design, development and implementation of secure routing in an open and distributed communication environments. Hence, this paper presents a enhanced novel approach to contribute the security goals where keys of source and destination nodes are shared through a alternative path such that nobody can misuse these keys.

The structure of the paper goes like this, section 2 briefs about recent research in security of MANETs communication. Detailed design and its implementation with results has been explained in section 3. Finally, section 4 concludes the paper and gives an outlook to further research.

II. LITERATURE SURVEY

The article[1] 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 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 DezertSmarandache theory applicability for trust assessment in mobile hostile environment.

Preeti and Sumitha [2] has analysed the MANETs in terms of security issues that are currently faced by the network including Bioinspired 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 [6] 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.

Shakshuki et al. [5] 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 to develop proficient intrusion detection mechanisms to safeguard MANET from attacks with the developments of the technology and cut in hardware costs.

Manuscript received October, 2013.

Chandrakant N, Dept of CSE, UVCE, Bangalore University, Bangalore, India,

To regulate such kind of movement, they muscularly believed that it is essential to address its potential security issues.

Paper [7] 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 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 itself against both malicious and unauthenticated nodes with marginal performance variation.

In paper [8], highlighted adhoc 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. These stuff also affects the existing security schemes for wireless networks which makes them much more susceptible to security attacks.

Tamilarasi, et al. [9] 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.

Paper [4] 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.

III. DETAIL DESIGN

In this network, source node will generate a key called KEY2 and destination node will generate a key called KEY1. When source node initiates communication for destination , it will send a request packet to destination via shortest/less cost path(PATH1). Here PATH1 can have many nodes and each node will generate a secret key whenever it receives a packet for first time for a particular session. Now that packet should take this key and move ahead to next node , similarly , next node too generates a secret key and appends to this packet, this task will be continued until packet reaches its destination, these all intermediate keys(IK) are merged(like applying arithmetic or logical operation) to form a unique key in the destination called as IKn2 where n>2 i.e. excluding source node and destination node. Both side communications should have respective node's keys. i.e. source packet should have KEY1,IKn2 and destination packet should have KEY2,IKn2. KEY1, KEY2 and IKn2 will expire after each session ends. So keys are shared before communication establishment.

Algorithm 1 *main()*

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

```
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:    path1 = generateShortestPath(src,dst)
12:    path2 = generateRandomPath(src,dst)
13:    acknowledgement1=initializeCommunication(src,dst,
       path1);
14:    acknowledgement2=initializeCommunication(dst,src,
       path2);
15:    acknowledgement3=initializeCommunication(src,dst,
       path2);
16:    if acknowledgement1 contains key =
       IKn-2 ) then
17:      if acknowledgement2 contains key =
         key1 ) then
18:        if acknowledgement3 contains key =
           key2 ) then
19:          proceedCommunication(src,dst,path1)
20:        end if
21:      end if
22:    end if
23:  else
24:    exit
25:  end if
26: end while
```

Destination will hold this packet and it will send a new request packet with KEY1(which is generated by source with path IKn2) to source node via different path other than the received packet's path(PATH2)to cross check the request of source. After source accepting this packet, it will send only KEY2 to destination again through same path(PATH2). When destination node validates the request and if it is satisfied with all measures, then it goes for communication. Now destination and source proceeds with usual communication bydecrypting data using 3 keys (KEY1,KEY2 and IKn2 via previous path(PATH1). Here both side communication should have respective node's keys. i.e. source packet should have KEY1,IKn2 and destination packet should have KEY2,IKn2. KEY1, KEY2 and IKn2 will expire after each session ends. So keys are shared before communication establishment.

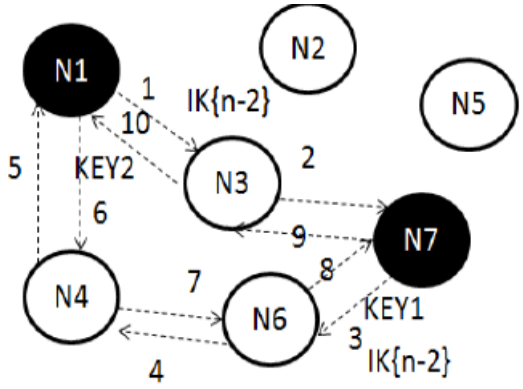

Figure 1. Sample Nodes Communication

The example of communication is shown in Figure 1 In the figure, N1(src) wants to send a RReq packet to N7(dst). N1 sends RReq packet to N3, and N3 sends same to N7 with its own generated key called IK1(IKn2,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 key 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 for 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 each session ends between nodes. KEY1, KEY2 and IK1 will be stored in N1, N7 until the session of communication ends, then this key will be invalidated. 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 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 2.

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.

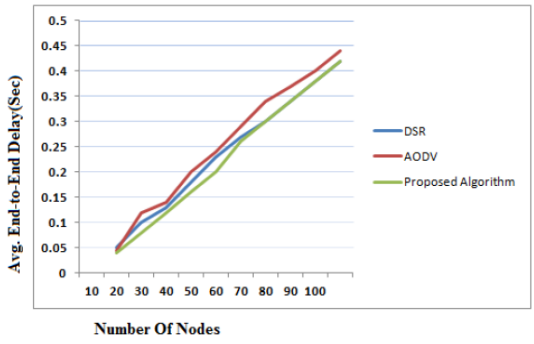

Figure 2. End-to-end delay of DSR, AODV and Proposed Algorithm

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 our 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. CONCLUSIONS

A novel approach has been presented in this paper where generated keys are used to communicate each other by exchanging them via unusual paths(other than shortest path). Here, one of the important thing is to have a unique for a particular path and both side parties should have their keys i.e. source packet should have KEY1,IKn2 and destination packet should have KEY2,IKn2. KEY1, KEY2 and IKn2 will expire after each session ends. The simulation results and consistency of algorithm have encouraged this paper to expose on WWW ! This idea can be further improved to support multikey for both paths (PATH1 and PATH2)so that security is much more stronger.

REFERENCES

1. 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.
2. 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.
3. 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.
4. 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.
5. Shakshuki, E.M. and Nan Kang and Sheltami, T.R. Eaack:a secure intrusiondetection system for manets. volume 60, pages 1089–1098, 2013.
6. L. ShiChang, Y. HaoLan, and Z. QingSheng. Research on manet security architecture design. In Signal Acquisition and Processing, 2010. ICSAP '10. International Conference on, pages 90–93, 2010.
7. S. Soni and S. Nayak. Enhancing security features amp; performance of aodv protocol under attack for manet. In Intelligent Systems and Signal Processing (ISSP), 2013 International Conference on, pages 325–328, 2013.
8. S. J. Sudhir Agrawal and S. Sharma. A survey of routing attacks and security measures in mobile adhoc networks. In JOURNAL OF COMPUTING, VOLUME 3, ISSUE 1, ISSN 21519617, pages 41–48, 2011.
9. Tamilarasi, M. and Sundararajan, T. V P. Secure enhancement scheme for detecting selfish nodes in manet. In Computing, Communication and Applications (ICCCA), 2012 International Conference on, pages 1–5, 2012.