POWER AND TRUST BASED SECURED ROUTING APPROACH IN MANET

[1]Arnab Banerjee, [2]Aniruddha Bhattacharyya, [3]Dipayan Bose

Department of Computer Science & Engineering, Institute Of Engineering & Management, Saltlake, India
[1]arnab.saheb@gmail.com
[2]aniruddha.aot@gmail.com
[3]connect2dipayan@gmail.com

ABSTRACT

Security in MANET has been one of the most highly rated issues in research field for the last few decades because of its self organizing and cooperative nature, capable of autonomous operation, rapid changing topologies, limited physical security and limited energy resource. So to combat with the security attacks against mobile ad hoc networks we propose a new scheme significantly differing from other existing schemes. In this paper, our proposed scheme, Efficient Secure Routing Protocol in MANET (ESRP) provides a new routing scheme based on trust, an integer value, helping in the selection of administrator inside the network for routing. The comparison between our proposed protocol and other existent secure protocols shows an enhanced and improved performance of our protocol based on the mobile ad hoc parameters. We have also implemented the message confidentiality and integrity in our proposed scheme. Our simulation result shows the robustness, reliability and trustworthiness of our scheme

KEYWORDS

MANET, willingness function, ESRP, trust, administrator

1. INTRODUCTION

A mobile ad-hoc network (MANET) is a self-configuring network consisting of mobile hosts equipped with wireless communication devices. The transmission of a mobile host is received by all hosts within its transmission range due to the broadcast nature of wireless communication and omni-directional antennae. If two wireless hosts are out of their transmission ranges in the ad hoc networks, other mobile hosts located between them can forward their messages, which effectively build connected networks among the mobile hosts in the deployed area. Due to the mobility of wireless hosts, each host needs to be equipped with the capability of an autonomous system, or a routing function without any statically established infrastructure or centralized administration. The mobile hosts can move arbitrarily and can be turned on or off without notifying other hosts. The mobility and autonomy introduces a dynamic topology of the networks. Ad Hoc networks are new paradigm of wireless communication for mobile hosts where node mobility causes frequent changes in topology. It has been used in a wide range of applications ranging from a battlefield to the user’s living room. Many efficient routing protocols have better network performance however they are more vulnerable to security threats. Ad hoc network has faced even more serious security problems as compared to traditional wireless networks. Several security solutions require a centralized server for key distribution or a secret

DOI : 10.5121/ijsptm.2012.1304

understanding between communicating entities. This lack of infrastructure has posed serious threats as far as routing security is concerned. Secondly, the vulnerability of the nodes towards physical compromise gives rise to serious internal threats within the network which make the issues of authentication, integrity and confidentiality even more challenging than conventional wireless networks. Thirdly, without support from fixed infrastructure it is undoubtedly arduous for people to distinguish the insider and outsider of the wireless network thereby difficult to tell apart the legal and illegal participants in wireless network. This assumption is also coupled with pre-configuration of nodes with encryption keys prior to joining the network. Public key cryptography with digital signature makes the network stronger to stand up against the attackers and secure communication is assured. However, due to the limitation of battery energy of mobile nodes, methods of prolonging the lifetime of nodes as well as the network become the key challenge in MANET. The performance of MANET depends on the routing scheme employed and the traditional routing protocols do not work efficiently in MANET. Developing routing protocols for has been an extensive research area in recent years, and many proactive, reactive and hybrid protocols have been proposed from a variety of perspectives[1]. Section I introduces our research on the security of MANET. Section II describes the Working Methodology of ESRP, while section III explores related works in this domain. Section IV describes our proposed algorithm. In section V, we present the proposed packet format while section VI gives us the picture of the performance evaluation. Lastly, section VII deals with all future work and section VIII express the conclusion in relation to this domain.

2. WORKING METHODOLOGY OF ESRP

Our proposed routing algorithm, ESRP (Efficient Secure Routing Protocol) is a pro-active routing protocol inspired by OLSR [2]. In this algorithm trust has been established using signed acknowledgement based on asymmetric key cryptography. Key distribution is out of the scope of this paper and any popular key distribution methodology can be followed. This protocol concentrates in dispersal of packets from source to network through administrator. We have selected Admin node as a minimal subset of all nodes that can form a fully connected network. It consists of all the administrators which can reach out to all the neighbor nodes. This administrator node selection depends on symmetric link, node coverage, willingness of that node and TRUST.

3. RELATED WORKS

Till date many secure routing protocols have been developed like SOLSR, TAODV, SAODV, etc. SOLSR [3] (based on OLSR) has used symmetric key for encrypting all data and control packets but Trust concept has not been implemented yet. While TAODV [4] (based on AODV [5]) does not use any encryption technique but it uses the trust factor. Again when considering the case of SAODV [6], it uses public key cryptography and digital signature to protect RREQ & RREP messages [7]. It also uses hash-chain to authenticate hop-count of each message. Few secured routing protocols like SRP [8], FTAODV [9], Ariadne [10] and others [11], [12], [13] have similar kind of approaches and so are not included in this paper. So in our protocol we have blended the concepts of both cryptography and trust factor to enhance the security of the protocol. We are using digital signature in each acknowledgement packet to prevent generation of forged packet.

4. PROPOSED ALGORITHM

This paper outlines the mechanism for selection of administrator, based on willingness & trust value of a node considering more exhaustive parameters so as to keep the admin node count to the minimum (as per basic OLSR) and make routing more secure. Our algorithm forces the same path return as traversed while sending. Only when absolutely necessary, admin node can switch from one node to another, offloading their job to the other node, increasing network runtime. The algorithms to maintain a secure and reliable network run in each individual node.

First we will discuss about Admin node selection algorithm. The value of willingness will be derived from next algorithm and trust from algorithm given in section 4.

4.1. Dynamic Willingness Function

Our algorithm takes a weighted sum of battery power of a node, coverage area and reliability of the node while calculating willingness value. The weighted values are experimentally tested and optimized. The power factor in MANET is crucial so it has been assigned the highest weighted value and so on. All weights are experimentally tested and optimized value for the scheme.

Willingness (P, C, R) = (0.75 * P) + (0.15 * C) + (0.1 * R) **(1)**

Where, P: power available for that node (in %)

P = (current node power/rated capacity of the node)*100 **(2)**

C: coverage (in %)

C = (no of 1-hop neighbors of that node / no of 2-hop neighbors of nodes that want to select this node as its ADMIN)*100 **(3)**

R: reliability of the node (in %)

Reliability (R) is calculated from various sensor inputs regarding outside environment condition where R ranges from 0% to 100% depending upon the node’s position. R = {0% … 100%} **(4)**

4.2. Admin Node Selection

This algorithm selects the administrator node which can cover most of the 2-hop neighbor of its selector. Selection also takes care of willingness and trust value of node. In case of tie, node with higher trust/power will be selected.

4.2.1. Few Definitions

- ADMIN(x): Admin set of node x which is running this algorithm.
- N1(x): One hop neighbor set of node x (symmetric neighbors)
- N2(x): Two hop neighbor set of node x [symmetric neighbors of nodes in N(x)].The two hop neighbor set N2(x) of node x does not contain any one hop neighbor N(x) of node x.
- D(x,y) : Degree of one hop neighbor node y (where y is a member of N1(x) -- means y belongs to N1(x)), is defined as the number of symmetric one hop neighbors of node y EXCLUDING the node x and all the symmetric one hop neighbors of node x, i.e.,
  D(x, y) = N(y) - {x} – N1(x) **(5)**
- W = Current willingness value of the node. [can range from 0 to 7]

- T = Current trust value of the node. [can range from 0 to 10]

  Trust_Threshold = Implementation dependent [we choose 2]

4.2.2. Initialization

1. Initialize Node_Trust table with default trust value 3 for each node.
2. Initialize PATHLIST = [].

4.2.3. Algorithm

Step 1: Start with an empty ADMIN(x) set.

Step 2: Calculate D(x, y), where y is a member of N1(x), for all nodes in N1(x) (put for all +ve sign)

Step 3: First select as ADMINs those nodes in N1(x) which provides the "only path" to reach some of the nodes in N2(x). [Trivial case]

Step 4: For each node in N1(x)

```
    {
    4.1 SELECT current node as a ADMIN as per table 1.
    4.2 While if some nodes still exists in N2(x) that is not covered by ADMIN(x):
    {
        For each node in N1(x), calculate the no. of nodes in N2(x) which are not yet covered by ADMIN(x) and are reachable through this one hop neighbor of x.
    }
    4.3 Select as an ADMIN that node of N1(x) which reaches the maximum number of uncovered nodes in N2(x) & refer table 1.
    4.4 If a tie occurs, select that node as ADMIN who’s D(x, y) is greater & refer table 1.
    }
```

Step 5: To optimize, process each node y in ADMIN(x), one at a time, if ADMIN(x) - {y} still covers all nodes in N2(x) then remove y from ADMIN(x).

Step 6: After that Convert the link between node x and ADMIN as SYM_LINK to ADMIN_LINK

Step 7: Exit

4.2.4. Table

Table 1: Admin Selection in case of tie

NODE 1:				
TRUST (T1) %	POWER (P1)%	TRUST (T2) %	POWER (P2)%	SELECTION
L	L	L	L	WHEN BOTH THE NODES HAVE THE SAME VALUES *THEN* SOURCE NODE CAN BROADCAST THE MESSAGE TO THE NETWORK THROUGH EITHER OF THE NODES. EITHER NODE1 OR NODE2
L	L	L	H	NODE2
L	L	H	L	NODE2
L	L	H	H	NODE2
L	H	L	L	NODE1
L	H	L	H	(IF P1>P2 THEN NODE1 ELSE NODE2) *ELSE* (IF P1==P2 THEN IF T1>T2 *THEN* NODE1 ELSE NODE2)
L	H	H	L	(IF P1-TH_PWR>T2-TH_TR & T1-TH_TR > P2-TH_PWR *THEN* NODE1) *ELSE* (IF T2-TH_TR>P1-TH_PWR & P2-TH_PWR > T1-TH_TR *THEN* NODE2)
L	H	H	H	NODE2
H	L	L	L	NODE1
H	L	L	H	(IF P1>P2 *THEN* NODE1 *ELSE* NODE2)

H	L	H	L	(IF T1>T2 & P1-TH_PWR>P2_TH_PWR *THEN* NODE1) *ELSE* (IF T2>T1 & P2-TH_PWR>P1_TH_PWR *THEN* NODE2)
H	L	H	H	NODE2
H	H	L	L	NODE1
H	H	L	H	NODE1
H	H	H	L	NODE1
H	H	H	H	(IF P1>P2 THEN NODE1 *ELSE* NODE2)

4.3. Digital Signature and Trust Value Calculation

4.3.1. Sender Node's Job

Step 1: Encrypt the message with Public Key of destination
ENC_MSG←ENCRYPT (PlainText_MSG)

Step 2: Calculate HASH VALUE for ENC_MSG
HASH_VAL ← HASH (ENC_MSG)

Step 3: Create a entry for PATHLIST table with following data:
< HASH_VAL, DEST_NODE_ID >

Step 4: Set a TIMER for this entry with timeout value T.
[Value of T is implementation dependent]

4.3.2. Original Message Passing

4.3.2.1. If the Node is Intermediate Node

Step 1: Receive the encrypted message.

Step 2: Append next Hop ID to the variable Path.

Step 3: Update the packet size to reflect the modified Path**.**

Step 4.1: Calculate: HASHVAL←HASH (MSG.ENC_MSG)

*Step 4.2***:** Store the following entry in PATHLIST table:

<HASHVAL, DEST_NODE_ID +MSG.PATH>

```
Step 5:   Set TIMER with T sec Timeout for this entry.

Step 6:   Forward the updated encrypted message.
```

4.3.2.2. If the intended Node is Receiver Node (DEST)

```
Step 1: Extract PATH from received message:
        PATH ← MSG.PATH

Step 2: Extract message:
        MSG←DECRYPT (MSG.ENC_MSG)

Step 3: Create a HASH value for ACK message generation:
        HASHVAL_C←HASH (MSG.ENC_MSG)

Step 4: Sign the ACK message:
        SIGN← ENCRYPT (HASHVAL_C, PVT_KEY_DEST)

Step 5: Transmit the ACK message with SIGN to Previous Node found in PATH.
```

4.3.3. For Acknowledgement Message

```
Step 1: Receive the ACK packet.

Step 2: Extract the encrypted hash value.

        HASHVAL_R←ACK.ENC_HASH
        [Where ACK.ENC_HASH = ENC (HASH (ENC_MSG), PRK_DEST))]

Step 3: Find entry in PATHLIST with HASHVAL_R

Step 4.1: If entry found

        i)      Extract stored path:  E_PATH ←Entry. PATH
        ii)     If the last node in E_PATH is Sender Node of this ACK packet
                then
                 increase TRUST of Sender Node by 1.
                Else
                decrease TRUST of Sender Node by 1 and discard the packet.
                Remove this entry from PATHLIST.
                Round off TRUST to within 0 to 10.
                GOTO Step 5
        iii)    Update the E_PATH of ACK packet by removing the Sender Node ID.
                Remove this entry from PATHLIST.
        iv)     Forward the ACK message to the previous hop in E_PATH.
        v)
Step 4.2:  If entry not found decrease TRUST of Sender node by 1(round off within 0 to 10) and
           discard the packet.
           Remove this entry from PATHLIST.
           GOTO Step 5

Step 5:   Done.
```

4.3.4. On expiration of time out for particular entry in path list

Step 1: Extract path from Time out entry:
PATH_T ← Timeout_Entry.PATH

Step 2: Decrease TRUST value for last node in PATH_T by 1unit

Step 3: Remove the entry from PATHLIST table.

5. Packet Format

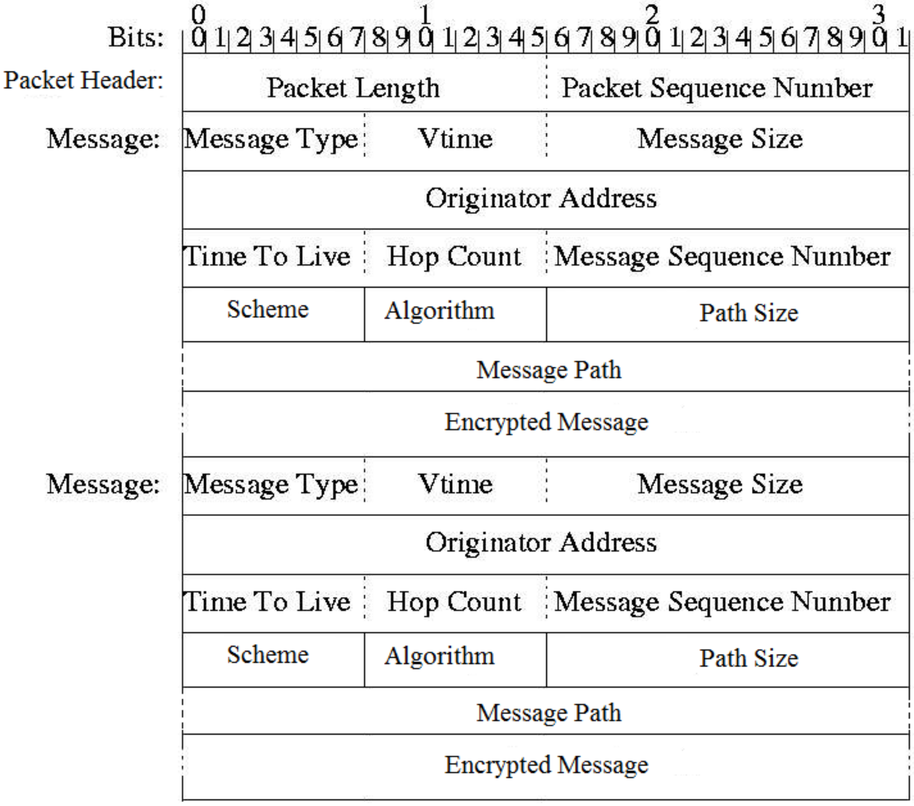

Figure 1: MESSAGE PACKET FORMAT

As multiple packet are piggybacked (as in OLSR) into a single packet, each message part will contain its own path and separate encrypted message content. All message type except HELLO_MESSAGE will be encrypted with destination node's public key. Scheme & Algorithm field is used to send ATSR specific data. In each hop, Message Path field is updated to add the current hop address. Accordingly, Message Size & Packet Length is updated. For ACK packet (Message Type = ACK), Message Path is omitted for ACK packet. Instead of Encrypted Message part, following is send:

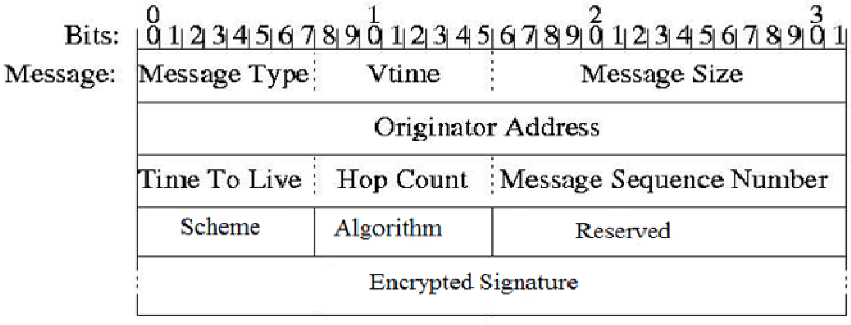

Figure 2: ACK PACKET FORMAT

6. Performance Evaluation

6.1. Admin Node Selection

We used OLSR protocol implementation from Niigata University for Glomosim [14] [15].

Parameter	Value
Terrain Dimension	(600x500) sq. meter
Simulation Time	500 minutes
Channel	Noisy
Noise Figure	10 dB
Radio Frequency	2.4 Ghz
Radio Receive Threshold	-65.046 dBm
Radio Transmit Power	22.5 dBm
Node Placement	Random
Mobility Speed	0-10 m/s
MAC Protocol	802.11
MAC Propagation Delay	1000 ns
Bandwidth	11 Mbps
Routing Protocol	OLSR, ESRP, SAODV
Number of Interface per node	2
Rated Battery Power (each node)	1500 mAh
Data Packet Type	FTP, CBR
Data Packet Size	2044 byte
Cryptographic algorithm	RSA (512 bit)

Table 2: SIMULATION PARAMETRES

To simulate the proposed algorithm we used Glomosim 2.03 network simulator [14]. Glomosim can simulate both wired and wireless network with layered TCP/IP stack with model based on noisy & noiseless channel with MAC protocol 802.11/CSMA/MACA/TSMA and various network, transport & application layer protocols. Glomosim is written using PARSEC language [16], a C derivative for large scale parallel simulation.

6.2. Energy Consumption Model

We are using IEEE 802.11b (DSSS modulation) as MAC protocol. The transceiver uses energy both to transmit and to listen for incoming packet. It also consumes energy in idle state. Let, the energy needed to transmit a packet E_t for duration t_t and to receive a packet E_r for duration t_r .Also assume it waits for t_i consuming energy E_i . Then total energy consumed by that node will be approximately:

$$E_c = E_t * t_t + E_r * t_r + E_i * t_i \qquad \textbf{(6)}$$

We assumed each node will use 5V DC battery with rated capacity of 1500 mAh. Transmission energy consumed will depend on radio signal strength of transmission; here we assumed 22.5 dBm; which approximately translate into 177.83 mW.

$$A = \frac{W}{V} \qquad (\textbf{7})$$

From equation (7) we get, A= 35.57 mA for V=5V DC. If we draw the same amount of current, using 1500 mAh battery, we'll get approximately 42 hour of runtime before the battery dies. Adding Idle and receiver power we'll get less than that.

6.3. Simulation Results

We have made a comparative study between OLSR, SAODV and our protocol ESRP. We carried out the result is based on the simulated data, the ACK being sent and frequency of data transfer. First we evaluate number of admin in the network by both protocols variant as a function of number of nodes. Maximum numbers of nodes were set to 50. Also to simulate attack vector, we configured Glomosim in such a way that 20% of those nodes will randomly drop packet or delay the delivery to next hop.

Simulation results are illustrated in following figures:

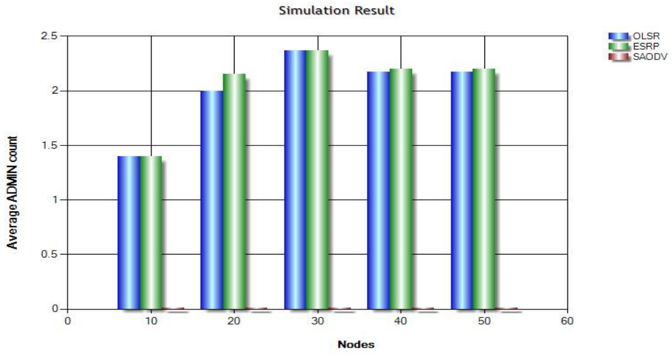

Figure 3: Admin Count

Here we can't see much difference in average ADMIN count over basic OLSR protocol. We can also see that number of ADMIN count has increased slightly when numbers of nodes were 20, 40 & 50. This increase in ADMIN count is due to shift in responsibility as the node's willingness & trust changes with time. Significant increase in ADMIN count adversely decreases network performance. But here the count has increased only slightly. SAODV does not use ADMIN concept. But increase in ADMIN count will affect radio layer packet collision, as depicted in figure 3.

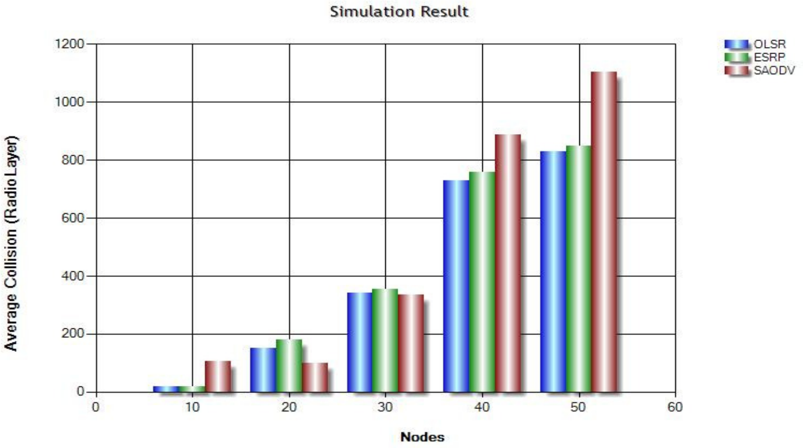

Figure 4: Average Collision

We can see the collision in fact has increased, but only slightly as the increase of ADMIN count was not so drastic. This increase was due to reselection of ADMIN and subsequent topology message being broadcasted internally. It also increases due to sending and receiving of acknowledgement packets. For SAODV, the increase in collision is due to frequent route request-reply in each transmission. Collision increases with network density as more and more nodes are trying to compete for radio frequency. Using 802.11b reduced collision due to deliberate use of collision avoidance scheme (such as RTS/CTS) built into radio layer protocol itself. Also we saw a slight change in throughput in the protocol. SAODV's performance was poor as compared to OLSR & ESRP. [Depicted in following figure]:

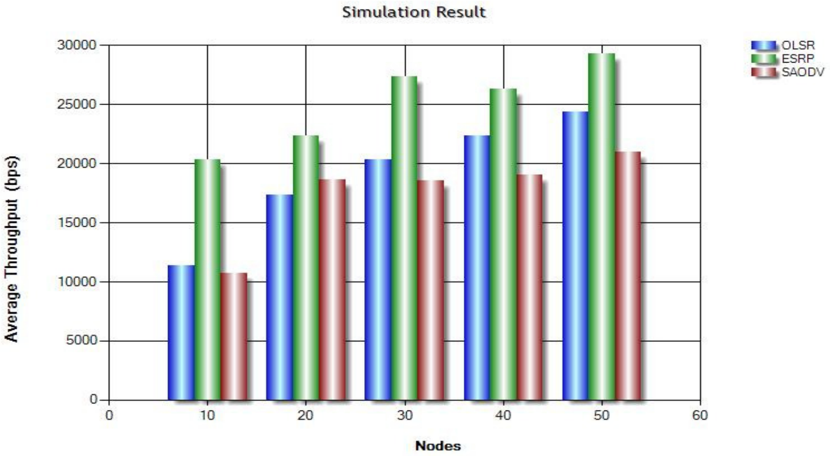

Figure 5: Average Throughput

With 11 Mbps network bandwidth and multiple FTP and CBR data transfer, we saw average throughput stayed around 27 kbps. Actually the average throughput increases in the case of successful data transfer. Implementation of security helps us to avoid retransmission of packets as well as data packet flooding. We also found that end-to-end delay also increased with our proposed protocol compared to stock OLSR:

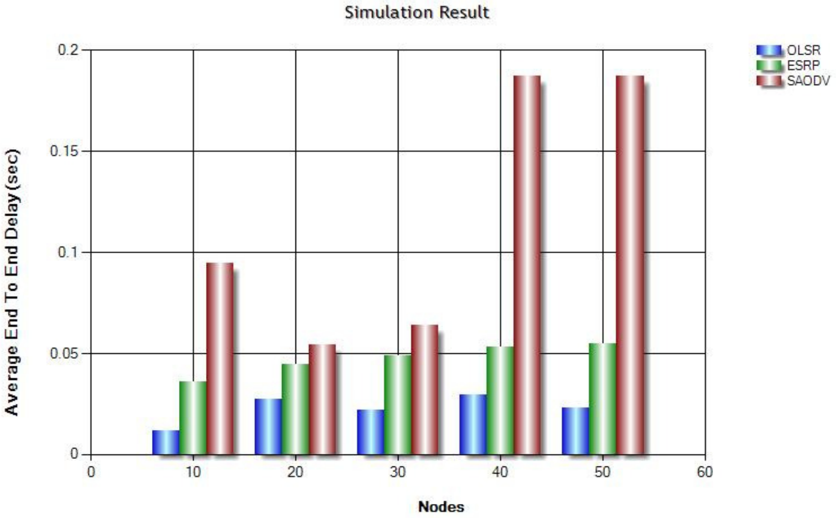

Figure 6: Average End-to-end Delay

Compared to ESRP, SAODV has increased end-to-end delay; we suspect it is due to transmission through suboptimal path. End-To-End delay increases for encrypting each message though the transmission of every packet is secured. Then ACK transmission and encryption of messages also increases the end to end delay considerably [17].

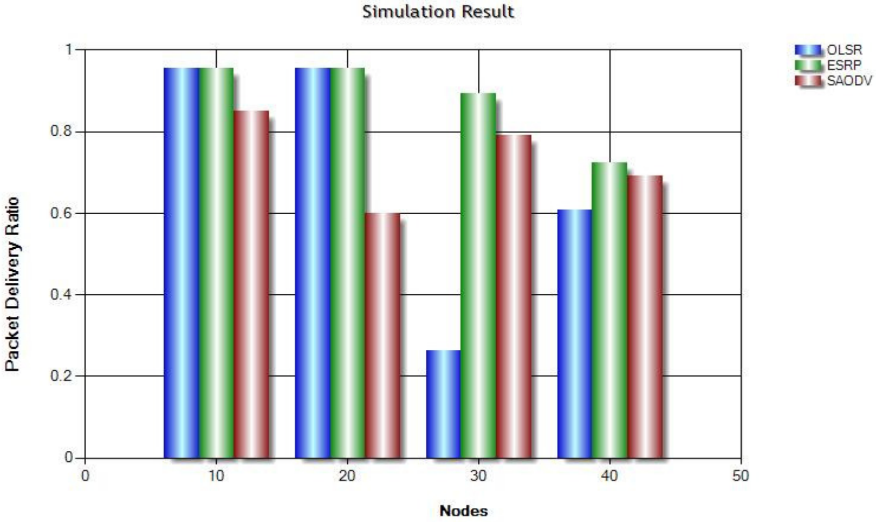

Figure 7: Packet Delivery Ratio

Compared to OLSR and SAODV the packet delivery ratio in case of ESRP has scored over with increase of the number of nodes. Though the packet delivery ratio of ESRP and OLSR scored nearly the same when the no. of nodes were 10 and 20 respectively, but steadily it rose with the increase in the number of nodes.

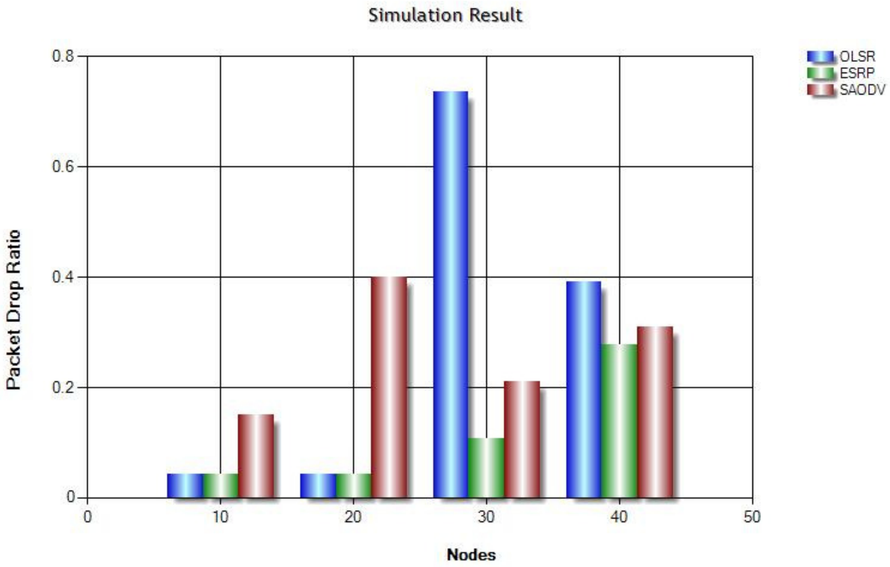

Figure 8: Packet Drop Ratio

From the figure 8, we see that when compared with OLSR, ESRP produces the same packet drop ratio when the numbers of nodes are 10 and 20 respectively but it produces better result than SAODV for the same number of nodes. With the increase of the number of nodes ESRP has more prominently produced better results than OLSR and SAODV.

We are trying to demonstrate that our protocol does not adversely affect the network performance compared to the existent solutions. Our protocol is quite robust as it protects from data and control traffic attacks.

7. FUTURE WORKS

Having already implemented the trust factor in ESRP, using signed acknowledgement which has enhanced the security of the routing protocol, we are also strongly working on the reliability factor of willingness function having already completed working on the power and coverage factors. We also have been able to successfully mitigate black hole, gray hole, forged ACK, snooping attacks using this protocol. Now our next future goal is to mitigate as many routing attacks as possible by simulating each of those attacks individually.

8. CONCLUSION

Our secure ESRP which is inspired from OLSR may not be energy efficient but is quite secure for end to end communication as compared to other routing protocols. In this paper Administrator as well as trust based routing has been proposed. This novel feature allows us to forward the data packets to the destination and by receiving the acknowledgement it verifies the validity of the nodes in the route. The performance of this routing algorithm in comparison to OLSR has improved. The security implementation has also protected the network from internal and external threats.

ACKNOWLEDGEMENTS

We are very thankful to Prof. Himadri Nath Saha and Dr. Prof. Debika Bhattacharyya who have guided us through the course of our work

REFERENCES

[1] Saoucene Mahfoudh, Pascale Minet, "An energy efficient routing based on OLSR in wireless adhoc and sensor networks", 22nd International Conference on Advanced Information Networking and Applications, 2008

[2] Workshops, 2008.T. Clausen, P. Jacquet, "Optimized Link State Routing Protocol (OLSR)", RFC 3626, http://http://tools.ietf.org/html/rfc3626

[3] Fan Hong; Liang Hong; Cai Fu; "Secure OLSR", 19th International Conference on Advanced Information Networking and Applications, 2005. AINA 2005. Page(s): 713 - 718 vol.1

[4] Xiaoqi Li; Lyu, M.R.; Jiangchuan Liu; "A trust model based routing protocol for secure ad hoc networks",Aerospace Conference, 2004. Proceedings. 2004 IEEE,Volume: 2, Page(s): 1286 - 1295

[5] C. Perkins; E. Belding-Royer; S. Das, "Ad hoc On-Demand Distance Vector (AODV) Routing." IETF. RFC 3561, July 2003

[6] Songbai Lu, Longxuan Li, Kwok-Yan Lam, Lingyan Jia; "SAODV: A MANET Routing Protocol that can Withstand Black Hole Attack",Conference on Computational Intelligence and Security, 2009. CIS '09, Page(s): 421 – 425

[7] Juwad, M.F.; Al-Raweshidy, H.S.; "Experimental Performance Comparisons between SAODV & AODV", Second Asia International Conference on Modeling & Simulation, 2008. AICMS 08, Page(s): 247 - 252

[8] Papadimitratos P., Haas Z. J., Samar P., “The Secure Routing Protocol (SRP) for Ad Hoc Networks”, draftsecure-routing-protocol-srp-00.txt, September 2002.

[9] J. Martin Leo Manickam, S.Shanmugavel, "Fuzzy based Trusted Ad hoc On-demand Distance Vector Routing Protocol for MANET", 15th International Conference on Advanced Computing and Communications, 2007

[10] Y.C. Hu, A. Perrig, and D.B. Johnson, “Ariadne: A Secure On- Demand Routing Protocol for Ad Hoc Networks,” Proceedings on Eighth Annual Int’l Conf. Mobile Computing and Networking (MobiCom), 2002, pp. 12-23.

[11] YANG Ya-tao, YUAN Zheng, FANG Yong and ZENG Ping, "A Novel Authentication Scheme Based on Trust-value Updated Model in Adhoc Network", 31st Annual International Computer Software and Applications Conference(COMPSAC 2007), 2007

[12] Raquel Lacuesta Gilaberte, Lourdes Peñalver Herrero, "A secure routing protocol for ad hoc networks based on trust", Third International Conference on Networking and Services (ICNS'07), 2007

[13] Jesus M. Gonzalez, Mohd Anwar, James B.D. Joshi, "Trust-based Approaches to Solve Routing Issues in Ad-hoc Wireless Networks: A Survey", 2011 International Joint Conference of IEEE, TrustCom-11/IEEE CESS-11/FCST-11

[14] Xiang Zeng, Rajive Bagrodia, Mario Gerla,"GloMoSim: A Library for Parallel Simulation of Large-scale Wireless Networks", Workshop on Parallel and Distributed Simulation, May 1998

[15] Niigata University, Information & Communication Networks laboratory, “OLSR_Niigata”, http://www2.net.ie.niigata-u.ac.jp/olsr-e.php.

[16] Rajive Bagrodia, Richard Meyer, Mineo Takai, Yu-an Chen, Xiang Zeng, Jay Martin, Ha Yoon, "Parsec: A Parallel Simulation Environment for Complex Systems", October 1998

[17] Dipayan Bose, Arnab Banerjee, Aniruddha Bhattacharyya, Himadri Nath Saha and Debika Bhattacharyya, et al.: An Efficient Approach to Secure Routing in MANET, Advances in Intelligent Systems and Computing, 1, Volume 176, Advances in Computing and Information Technology, Pages 765-776, DOI: 10.1007/978-3-642-31513-8_78

Authors

1. **ARNAB BANERJEE**

Having completed B.Tech in Computer Science & Engineering from AIEM, Durgapur, he pursued M.Tech degree in Computer Science & Engineering Department from Institute Of Engineering and Management, Saltlake.While pursuing M.Tech, he have gathered a year experience in teaching in Institute Of Engineering and Management as Lecturer Trainee in the Computer Science & Engineering Department. His interest includes Algorithm, AI, Fuzzy Logic, Automata.

2. **ANIRUDDHA BHATTACHARYYA**

He did his B.Tech in Electronics & Instrumentation from Academy of Technology, Hooghly and his M.Tech in Computer Science & Engineering from Institute of Engineering & Management, Saltlake, Kolkata. He has worked in software development industry for more than 2 years. His interest includes software development, HPC/Parallel/GPU Computing, embedded system design & AI.

3. **DIPAYAN BOSE**

Having completed B.Tech in Computer Science & Engineering from AIEM, Durgapur, he pursuaded M.Tech degree in Computer Science & Engineering Department from Institute Of Engineering and Management, Saltlake. Has interest in networking operating system(LINUX) and Algorithm.