A Novel Multipoint Relay based Secure Routing in MANET

Himadri Nath Saha Dr.Debika Bhattacharyya Dr.P.K.Banerjee

IEM,Kolkata,WB IEM,KolaKata,WB JU,Kolkata,WB

him_shree_2004@yahoo.com, bdebika@yahoo.com, pkbju10@yahoo.com

Abstract— *Security in routing is a challenging issue in mobile ad-hoc (MANET) network because of its open nature, infrastructure less property, mobility and energy constraints. Messages typically roam in multi-hopped fashion and nodes may be powered by limited energy source and with limited physical security. So we proposed a new scheme which is significantly different from others available schemes to provide security during routing in mobile ad hoc networks. In this paper, our proposed scheme, Secure Multipoint Relay based Routing in MANET (SMRR) provides routing based on trust, which is an integer value that helps to select Multipoint Relay (administrator) inside the network for routing. We have also implemented the message confidentiality and integrity in our proposed scheme. Our simulation results show the robustness, reliability and trustworthiness of our scheme.*

Keywords- *MANET, SMRR, trust, administrator, digital signature, willingness function, olsr, secure routing*

I. INTRODUCTION

Mobile Ad hoc network (MANET) can operate in a self-organized and non predefined infrastructure. The nodes in such networks can communicate with each other through direct wireless links or multi-hop routing. 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 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, the next important characteristic of a mobile ad hoc network is that the topology of the network changes dynamically. Thus, any security model, based on a fixed architecture cannot be used in such a scenario. 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 MANET has been an extensive research area in recent years, and many

DOI : 10.5121/ijnsa.2012.4610

proactive, reactive and hybrid protocols have been proposed from a variety of perspectives[1]. In rest of the paper, Section II describes the Working Methodology of SMRR, 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.

II. WORKING METHODOLOGY OF SMRR

Our proposed routing algorithm, SMRR (Secure Multipoint Relay based Routing) is a pro-active scheme inspired by OLSR [2]. This algorithm uses signed acknowledgement (signing based on asymmetric key cryptography) to establish trust. Key distribution is out of the scope of this paper and any popular key distribution methodology can be followed. This scheme uses administrator to disperse all the packets to the networks through the next hop administrator. Admin node is 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 admin node selection depends on symmetric link, node coverage, willingness of that node & Trust. SMRR scheme not only encrypts Transport layer data but also control messages sent by SMRR itself. Application data and control traffic are handled in separate way.

III. RELATED WORKS

Till date many secure routing protocols have been developed. 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 scheme we have blended the concepts of both crytography and trust factor to enhance its security. We are using digital signature to verify each acknowledgement so forged packet generation is not possible.

IV. PROPOSED ALGORITHMS

In this paper, we are proposing few new mechanism for calculating administrator based on willingness & trust of a node by taking care of more exhaustive parameters so that numbers of admin nodes are kept to minimum (as per basic OLSR) and routing becomes secure. Our algorithm forces same return path as while in sending. Only when it is absolutely necessary, admin node can switch from one node to another, offloading their job to other one, increasing network runtime. Below are the important algorithms that *each node* runs individually to maintain a secure and reliable network.

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

A. Dynamic Willingness calculation:

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 battery power in MANET is crucial because more routing will result battery power depletion and node may stop working. So it has been assigned the highest weighted value. Coverage is next important factor because more coverage ensures better routing and third important factor is reliability which is very important for implementation.

Willingness (P, C, R) =

$$(0.75 * P) + (0.15 * C) + (0.1 * R) \quad (2)$$

Where,

P: power available for that node (in %)
C: coverage (in %)
R: reliability of the node (in %)

Power (P) is defined as:

$$P = (\text{current node power/rated capacity of the node})*100 \quad (3)$$

Coverage (C) is defined as:

$$C = (\text{no of 1-hop neighbors of that node / no of 2-hop neighbors of nodes that want to select this node as its ADMIN})*100 \quad (4)$$

Reliability (R) is calculated from various sensor inputs regarding outside environment condition. R ranges from 0% to 100% depending upon the node's position.

$$R = \{0\% \ldots 100\%\} \quad (5)$$

B. Admin Node selection:

This algorithm selects the administrator node which can cover most of the 2-hop neighbour 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.

*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.,

$$D(x, y) = N(y) - \{x\} - N1(x) \quad (1)$$

- **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]

Initialization:

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

Algorithm:

Step1: Start with an empty ADMIN(x) set.

Step2: Calculate D(x,y), where y is a member of N1(x), for all nodes in N1(x) (put for all +ve sign)

Step3: First select as ADMINs those nodes in N1(x) which provide 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
whose 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

NODE 1:		NODE 2:		
TRUST (T1) %	POWER (P1) %	TRUST (T2) %	POWER (P2) %	SELECTION
SPCL	SPCL	SPCL	SPCL	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) ELSE NODE1
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)

Table 1: Admin Selection in case of tie

C. Digital Signature And Trust Value Calculation

I) *Sender node' 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, CRNT_N_ID + MSG.PATH >**
Step 4: Set a TIMER for this entry with timeout value T.
[Value of T is scheme dependent]

II) *Original message (DATA)*

- *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 (a): Calculate
HASHVAL←HASH (**MSG**.**ENC_MSG**)
Step 4(b): Store the following entry in **PATHLIST** table:
<**HASHVAL, CRNT_N_ID+MSG.PATH**>
Step 5: Set **TIMER** with T sec Timeout for this entry.
Step 6: Forward the updated encrypted message.

- *If the Node is Intended 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.**

- *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 1
Step 3: Remove the entry from **PATHLIST** table.

III) *SMRR specific messages (CONTROL)*

- Sending HELLO, MID, TC Message

Step 1: Create message as per existing OLSR scheme.
Step 2: Before sending it to network layer (such as IP), message content is encrypted with current node's Private Key as per packet format shown in Fig 2. Scheme & Algorithm field are set as per chosen parameter.

- Receiving HELLO, MID, TC Message

Step 1: Receive encrypted message from network layer.
Step 2: Before processing the received packet it is decrypted using originator node's Public Key and original message format is restored. This message is processed and forwarded (encrypted) as per existing scheme.

- For Acknowledge 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 (a): 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**.

Step 4 (b): 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.

- 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 1
Step 3: Remove the entry from **PATHLIST** table.

V. PACKET FORMAT

Our scheme only works to create and maintain a valid route table in host Operating System. It is host Operating System's responsibility to correctly route the packet to actual destination (as in OLSR). SMRR specific messages are handled by SMRR Network layer module.

Application data are directly sent by IP layer (or any underlying Network layer protocol). But to calculate Trust value, we need to handle Application layer data coming from Transport layer separately by SMRR module. Transport layer data are encrypted in network layer with destination node's public key. In each hop, Message Path field is updated to add the current hop address. In receiver side, before sending the data to Transport layer, it is decrypted by destination node's private key and an ACK message is created from the received packet as per the above algorithm. Intermediate nodes can't decrypt the data packet as they don't know the private key of intended receiver node. Actual Transport layer data are packed as per following packet format:

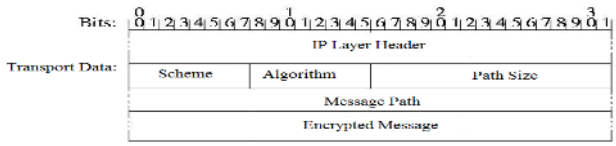

Figure 1: Data Packet Format

SMRR's native messages (i.e. ACK, TC, MID, HELLO) are sent/received & processed directly by SMRR module. As multiple SMRR messages are piggybacked (as in OLSR) into a single packet, each message part will contain separate encrypted message content. All message type except ACK_MESSAGE will be encrypted with originator node's private key. Scheme & Algorithm field is used to send SMRR specific data. Accordingly, Message Size & Packet Length is updated.

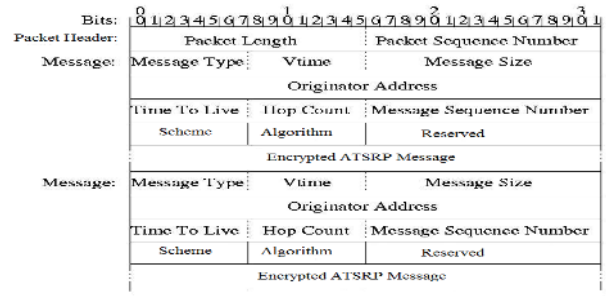

Figure 2: SMRR Message Packet Format

For ACK packet (Message Type = ACK) , instead of Encrypted Message part, signature is send:

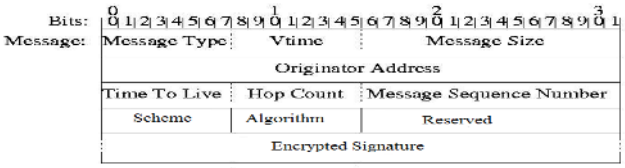

Figure 3: ACK packet format

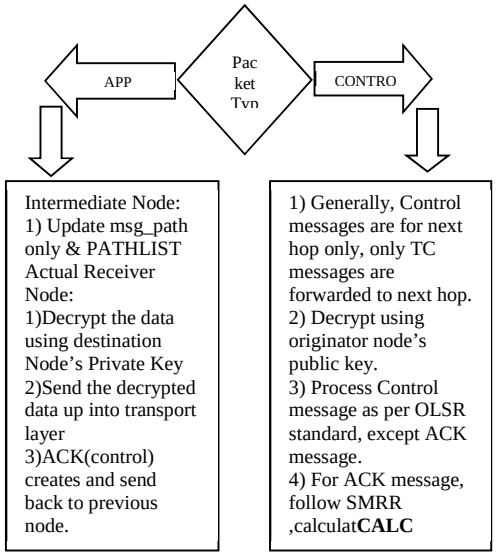

Figure 4: Flow of packets

VI. PERFORMANCE EVALUATION

A. Simulation Environment

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, SMRR, 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 parameters

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.

B. 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:

$$E_c = E_t * t_t + E_r * t_r + E_i * t_i \quad (6)$$

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.

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

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.

C. Simulation Results

We have made a comparative study between OLSR, SAODV and our scheme SMRR. 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 protocol 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:

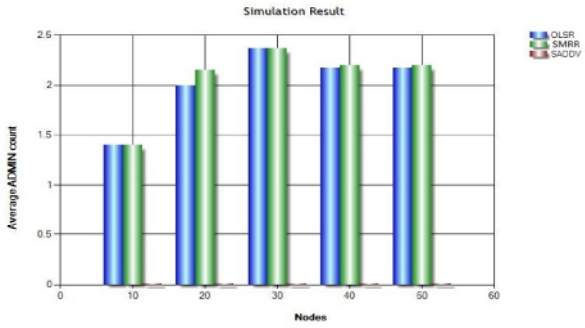

Figure 5: ADMIN Count

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. Increase in ADMIN count will affect radio layer packet collision as depicted in above figure5.

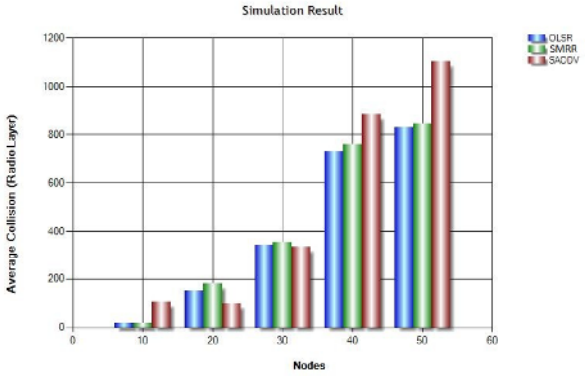

Figure 6: Average Collision

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 scheme. SAODV's performance was poor as compared to OLSR & SMRR as depicted in the above figure6.

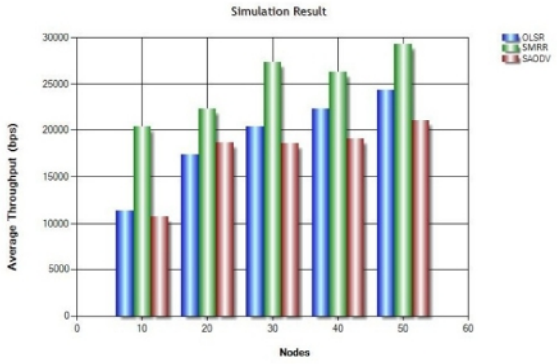

Figure 7: Average Throughput

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 scheme compared to stock OLSR as depicted in the above figure 7.

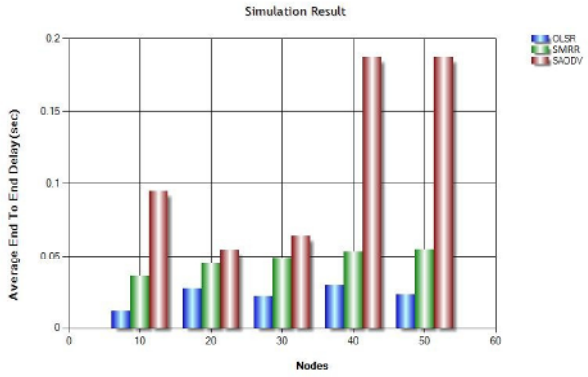

Figure 8: Average End-To-End Delay

Compared to SMRR, 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 as depicted in the figure8.

VII. FUTURE WORK

We have already implemented trust factor in SMRR using signed acknowledgement which has enhanced the security of the routing scheme. We have also been able to mitigate black hole, gray hole, forged ACK, snooping attacks using this scheme. We have also implemented parameterized willingness function in SMRR. Now our next future goal is to mitigate as many routing attacks as possible by simulating each of those attacks individually.

VIII. CONCLUSION

Our secure SMRR which is inspired from OLSR may not be energy efficient but is quite secure for end to end communication as compared to other routing scheme. In this paper Administrator and 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.

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