Circuits and Systems, 2016, 7, 1087-1097
Published Online May 2016 in SciRes. http://www.scirp.org/journal/cs
http://dx.doi.org/10.4236/cs.2016.77092

Scientific Research Publishing

Ant Routing Protocol with Location Services in Intermittently Connected MANETs

S. Ramesh[1], R. Indira[2]

[1]Department of CSE, Anna University, Regional Campus, Madurai, India
[2]Department of CSE, Adhiyamaan College of Engineering, Hosur, India
Email: itz_ramesh87@yahoo.com, indicse@gmail.com

Received 24 March 2016; accepted 24 May 2016; published 27 May 2016

Abstract

Wireless and mobile networks seem to deliver tremendous uses. In its way, MANET leads to enormous real world applications. Routing allows us to implement many real world applications. Complete affinity in an infrequent network like ICMANET is highly impossible. Disconnected MANET is also known as ICMANET which is also a DTN (Delay Torrent Network) that supports for higher delays. It is laborious process to execute routing in a diffused network process to execute routing in a diffused network. To deliver the data packets towards the destined node to its best, a new strategy in routing called Ant routing protocol in concoction with storage strategy LoDis has been proposed. Despite of routing, security is still an unsolved problem. To evaluate this situation, this paper presents a methodology called agent technology which yields a secure routing. Hostile node in the network is spotted with the help of agent at each node. A cryptographic algorithm Advanced Encryption Standard (AES) is habituated to improve secure communication in wide range Mobility and total number of nodes in the network act as variables in examining the hostile nodes in the network to judge the standard of security. Improved performance along with the security is the point to be highlighted.

Keywords

MANET, ICMANET, Delay Tolerant Network, ACO, A-LODIS, Agent, AES

1. Introduction

A group of independent mobile nodes connected via wireless medium is a MANET (Mobile Ad hoc Network). Here the nodes are arranged in a distributed manner. Message passing takes place with the help of the middle node between the source and the destination node. Wireless environment has a serious disadvantage in data

How to cite this paper: Ramesh, S. and Indira, R. (2016) Ant Routing Protocol with Location Services in Intermittently Connected MANETs. *Circuits and Systems*, **7**, 1087-1097. http://dx.doi.org/10.4236/cs.2016.77092

transmission so we have opted for the middle node.

It is studious to route in a temporary network topology. In the past ten years, innumerable conventional routing protocols namely distance vector, Link State Routing (LSR), Adhoc On demand Distance Vector (AODV), Distance Source Routing (DSR), Opportunistic Adaptive Routing, Open Shortest Path First (OSPF) routing have been propounded. Beneficial data communication has been promised in these routing protocols. Mobile connected via wireless medium is a MANET and a group of disconnected MANET is called as ICMANET.

Quintessential DTN (Delay Torrent Network) causes huge delays in ICMANET (Intermittently Connected Mobile Ad hoc Network). As confronted in infrequent communication or an interplanetary scale, ICMANET is sketched to execute beneficially over vast distances. High mobility of the nodes in the intermittent networks is a cause of infrequency within the wink of eye nodes getting agitated leads to coin of topology in a dynamic manner. Wild life tracking, habitat monitoring sensor network, military network, nomadic community network and vehicular network etc are some of the classic examples. Routing transforms to an arduous process because of classic contorted style of the network.

Since the past years number of routing protocols has been propounded for dissemation in ICMANET. Flooding, Epidemic, Direction Based Routing, Adaptive Routing, Utility Based Routing, Probabilistic Routing, Copy Case Routing, Spray and Wait Routing, LAROD etc. are some of the routing methodologies. These routing protocols follow a mode for data communication but security is still before question mark. Since MANET is idiosyncratic, the security issue in MANET is grounded to numerous technical disadvantages. Overhearing is due to an intermediate communication and also possesses more security in such case we go for IDS (Intrusion Detection System) by building a trust based environment. Intrusion Detection System has many diversity like behaviour based IDS, knowledge based IDS, Distributed IDS [1], Real Time IDS, Multi-layer Integrated Anomaly detection system, clustering approach; mobile based detection system co-operative approach etc. These known systems promise security in MANET.

As a result of disconnected behavior of the network of ICMANET, it cannot adopt security protocols sketched for MANET. IDS is the trust based system, which is in need of central serve to certify authentication. Since ICMANET don't have possibility to launch since these techniques are not suited. So a trending methodology for security should be sketched that is not in used for any central system.

In this paper, we recommend a new security protocol for ICMANET. Authentication terminology is passed to each agent at the nodes, the confronted node is promised to be the authenticated node. Before transmitting the data, it is encrypted. Advanced Encryption Standard (AES) is the algorithm used for ciphering and deciphering. This algorithm helps to ensure security without central server.

This paper is ordered as follows. Section II describes the related work for routing in ICMANET. The protocol terminologies are described in Section III. Section IV describes the procedure of secure routing. The execution examination is represented in Section V.

2. Related Work

Routing data packets is an uninteresting process in trending ICMANET. Impossibility of routing issue is worked and manifested in many research works. Routing methodologies that are applicable in intermittent network is bestowed in this section. The conventional routing protocol differs to a considerable extreme from new routing methodology. Considering the transient connectivity of ICMN the routing protocols should have the behavior of tolerating higher delays. Following is the detailed description of few intermittent routing protocols.

Flooding based routing is the classic scheme which acts as a platform for the schemes. Here, packet is sent from one node to all other nodes. Every single node is a propagator which attempts to move every message to one of its adjacent node as well as a receiver [2]. To deliver every message to all movable parts of the network is the expected yield. Conventional flooding based routing protocol is a platform for epidemic routing which states that periodic pair-wise connectivity is significant to deliver a message across the network [3]. Mobility of nodes within unique position of the network is a key for routing.

The beaconless routing protocol [4] is based on the theorem where on intervallic diffusion of beacons into the network doesn't exist. Moving nodes in a dispersed modus amidst its adjacent node is the initial step in routing without intellectuating the node detail. Asynchronous communication in ICMANET is brought into the forum by CAR algorithm, which acts as a platform for ordering messages in the network. Good delivery ratios and latencies with less overhead can be attained if nodes have the capability to view the node detail and make local decisions

prior to deliver a message [5] CAR need to predict and evaluate the node detail which results CAR (Context Aware Routing) to be a laborious process.

Scalable geographical routing is bestowed as a combination of gossip and random node mobility known as Brownian gossip [6]. Query related to other nodes information is move to each node along with certain values of probability. Information dissemination uses a gossiping technique which is done with probability namely *p* gossip to make the query to reach the secondary nodes in the network with highest probability is the promise made by probability value. A hub level routing method and two versions of user level routing methods are been labeled by the mobility profile base routing is maintained by a [7] SOLAR-HUB, which is involves routing.

Direction based geographic routing [8] is grounded towards the mean of geographical locations of packets that are routed that leads the path towards destination. When two nodes are interrupted current location, moving direction and the packets are interchanged. This is the point hypothesized in this algorithm. Selected nodes whose distance and moving receives the forwarded data packets. As the name specifies the single copy case routing [9] carries one copy of message packet to its sink node randomized routing, utility based routing, direct transmission seek and focus and oracle based routing are methodologies included *i.e.*, routing. Initially few copies of message are sprayed and individual sprayed copy is routed to the sink node is the methodology implemented in multiple copy case schema. Spray and wait and spray and focus are the two types of lemma in the multiple copy case routing [10].

To ensure static topology the network is divided into small parts and it upholds the detail regarding host mobility and connectivity changes for higher accuracy. This state's it as semi probabilistic routing algorithm [11]. The contention and dead end are considered for routing which is hypothesized in contention based routing [12], which yields the better performance in spray select and focus. Spray and hop phase [13] are the two phases of spray and hop routing protocol. The former sprays few copies of message to the network and the later happens after the initial phase only when node in spray phase was incapable to identify the sink. The spray and wait [14] scheme copies message and sprays into network and will be waiting till at least a single message copy reaches to its destinations. Easy execution and optimization to yield depicted performance is made possible.

Combination of beaconless routing protocol and storage forward carry technique is the LAROD-LODiS [15] routing in which routing is attained with the help of database. Constant overhead and higher delivery ratio is bestowed as a result of gossiping protocol. Though routing is made possible in ICMANET security is never taken into consideration in these techniques. To ensure security here we introduce the agent technology and AES (Advanced Encryption Standard) for an added security used with A-Lodis, routing protocol based on ACO (Ant Colony Optimization). Security in a system holds a significant responsibility to prevent vulnerabilities or data theft by the hackers.

3. Terminologies of Protocol

Terminologies that were revamped to ensure security in ICMANET is being potrayed in this section which is of A-LODis, Agent working, infrastructure and its concepts and general description of AES algorithm.

3.1. A-LoDiS Routing Protocol

Combination of optimization technique and gossiping technique is that an A-LOD is routing protocol. Formulation of ant working is been showcased here as a form of introduction. A well known problem solving technique is swarm intelligence [16], ACO is one of its phases. General habitat of bugs and other animals stands as a vision to develop swarm intelligence. In reference to this habitat of ant is taken as inspiration for ACO. It reaches its food by noticing the pheromone content in its way.

Deets transformation varying environment and local deets assessment by adjacent bugs are the two idiosyncrasy application in stigmergy mode of communication. ACO contains maximum number of ants that are required to get a solution for optimization problem. Most popular theory among ants is stigmergic mode of communication used for deets transformation. Wander mode, search mode, return mode, attracted mode, trace mode and carry mode are some of the foraging modes adopted by ants. Optimal solution is attained by supporting a collective interaction through indirect communication which is made possible by parallel and independent execution of ants. Thy individually move in its own way where it accumulates pheromone. The optimal path has more pheromone while less optimal way got its pheromone evaporated. Attractiveness, evaporation and pheromone are the three components of ACO. Beneficial method of bio-inspired communication is show cased in

ACO. Key features of ACO are as follows:

(i) Initialization
(ii) Traversing
(iii) Pheromone Deposition
(iv) Updating Pheromone

From **Figure 1**, it is clearly understood that the ant goes for optimal path to get its sink node is the point to be understood from the diagram 1. Pheromones deposited move in the path with frequent occurrences which is finalized as shortest path. A path where frequency of ant occurrences is less the pheromone gets evaporated. The algorithm starts with initializing the pheromone value. To finalize the optimal path from source to sink is done by generate solution function, followed by local search to get optimal path among from all paths. Pheromone values are updated after path determination. The algorithm for Ant is portrayed in **Figure 2** as follows.

3.2. Agent Technology

Agent is a set of rules which is capable to provide uninterrupted operation in a diligent environment. They are skilful to handle actions in flexible and highbrowed manners which are subject to changes in the environment. Agent is a piece of code in charge to perform the pre assigned chores. Agents' decision depends on its spontaneous proficiency and prior experiences [17].

Security check is done with certain agent parameters by agents placed at each node [18]. Parameters are in detail as follows:

(i) *Node ticket*—Unique ticket for each node in the network.
(ii) *Counter sign*—Open key for all nodes in the network.
(iii) *Mobility Model*—The mobility model of the network topology.
(iv) *Origin of Placement*—The initial placement of each node in the network.
(v) *Lattice Card*—An n × n matrix in which each lattice comprises a particular data in it. Each node contains a unique lattice.
(vi) *Archetype Generation*—The network is with some geometric figuration with which the node assimilates a solitary archetype.

These parameters accumulate on security issues linked in the ICMANET. Each node contains an agent comprises of these components namely:

(i) Data Aggregator
(ii) Node Scrutinizer
(iii) Information Telecaster

3.3. Data Aggregator

It has aggregate of detailed information about all nodes within the network. It contains agent parameters of every node.

Figure 1. Ant Movement from source to destination.

```
Initialize Pheromone Value
While (not termination)
   Generate Solution ()
   Local Search ()
   Pheromone Update ()
End While
```

Figure 2. The General Ant Algorithm.

3.3.1. Node Scrutinizer

It scrutinizes whether the node that receives information in a one among the topology. It chooses any one of agent parameter and checks with the accumulator for confirmation. If they don't match then it telecasts the presence of foreign node.

3.3.2. Information Telecaster

It acts as a mediator that allows access for communication among the encountered node. Routing is permitted only if it is confirmed as authorized node by scrutinizer. Execution of agent set at each node is clearly in **Figure 3**. When ancillary node receives a message from elementary node, it checks with node accumulator by any one of the agent parameter. Data aggregator is a database if emulate is identified then it is forwarded towards the data telecaster which authorize the node to transfer the message to the encountered node if not node scrutinizer telecasts the interrupt of foreign node within the network.

3.4. AES Algorithm

Security, cost and compactness and design and implementation simplicity are the key characteristics of AES. As known block size of 128,192,256 is supported by AES and a key size is 128 bits which could be varied depending upon the application. Unlike other encryption technique AES does not use multiple keys which made it to be simplified algorithm. Firstly the input data is transformed to a state array of 4 × 4 matrixes as shown below

$$\text{Input Block} = \begin{bmatrix} i0 & i4 & i8 & i12 \\ i1 & i5 & i9 & i13 \\ i2 & i6 & i10 & i14 \\ i3 & i7 & i11 & i15 \end{bmatrix} \quad (1)$$

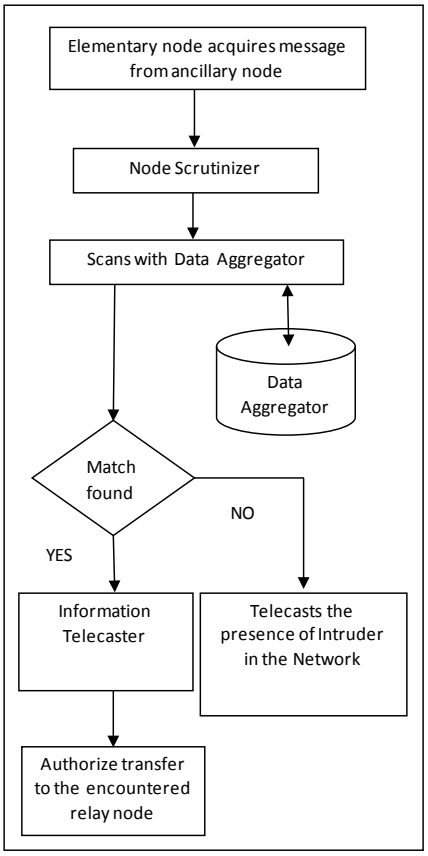

Figure 3. Agent execution.

Here $i0 \cdots i15$ indicates input data.

Similarly key is also transformed to 4 × 4 matrixes. Number of rounds in AES depends on the input size. Each round other than final round undergoes four evolutions as follows.

(i) Substitute Bytes
(ii) Shift Rows
(iii) Mix Columns
(iv) Add Round Key

The internal functions in AES uphold its operation on a finite field, the polynomials modulo over $f(x)$.

$$f(x) = x^8 + x^4 + x^3 + x + 1 \tag{2}$$

3.4.1. Substitute Bytes

A process of non-linear substitution on each byte of the state array is the substitution bytes. Table lookup method is the one where we use an S-Box to match value. Any non-zero byte X is substituted by following modification.

$$Y = Ax^{-1} + b \tag{3}$$

where A and b are constant 8 × 8 matrixes.

3.4.2. Shift Rows

This is nothing but the transposition cipher operates on each row of a state array [19]. For elements of i^{th} row, the position rearrangement is cyclic shift to right by $4 - i$ positions. It changes the position of elements as follows:

$$\begin{bmatrix} S0,0 & S0,1 & S0,2 & S0,3 \\ S1,0 & S1,1 & S1,2 & S1,3 \\ S2,0 & S2,1 & S2,2 & S2,3 \\ S3,0 & S3,1 & S3,2 & S3,3 \end{bmatrix} \downarrow \begin{bmatrix} S0,0 & S0,1 & S0,2 & S0,3 \\ S1,1 & S1,2 & S1,3 & S1,0 \\ S2,2 & S2,3 & S2,0 & S2,1 \\ S3,3 & S3,0 & S3,1 & S3,2 \end{bmatrix} \tag{4}$$

3.4.3. Mix Columns

This function on each column where each byte of a column is matched into a value, which is a function of all other, our bytes of that column, which is done by multiplying the state matrix and constant matrix.

$$C \cdot S = S' \tag{5}$$

where S = 4 × 4 matrix before transmission of Equation (4)
S' = Outcome f Equation (5)
C = Constant matrix

$$C = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \tag{6}$$

Single column transformation is shown below

$$
\begin{aligned}
S'0, j &= (2 \cdot S0, j) \oplus (3 \cdot S1, j) \oplus S2, j \oplus S3, j \\
S'1, j &= S0, j \oplus (2 \cdot S1, j) \oplus (3 \cdot S2, j) \oplus S3, j \\
S'2, j &= S0, j \oplus S1, j \oplus (2.S2, j) \oplus (3 \cdot S3, j) \\
S'3, j &= (3 \cdot S0, j) \oplus S1, j \oplus S2, j \oplus (2 \cdot S3, j)
\end{aligned} \tag{7}
$$

3.4.4. Add Round Key

A bitwise XOR operation takes place between elements of state array and round key. Except the final round all four transformation will happen in decryption too. Expanding the 128 bit key is a key expansion comprises of following steps:

(i) One-byte circular shift on a word.

(ii) A byte substitution on each byte of its input using *S*-box.

(iii) The results of previous steps are XOR ed with a round constant RC [*j*].

$$
\begin{aligned}
\mathrm{RC}[j] &= (\mathrm{RC}[j], 0, 0, 0) \\
\mathrm{RC}[1] &= 1; \mathrm{RC}[j] = 2 \cdot \mathrm{RC}[j-1]
\end{aligned} \tag{8}
$$

4. Routing Methodology

Secure communication in assistance with A-Lodis is explained in this section. When a node A tries to pass a message to node B it initially reaches the relay node if the sink node is not within its territory. Message is passed to relay node only after confirming it as an authorized node in the network. This checking process is done by agent technology. Each node comprise of an agent initiates to test R1. The scrutinizer of agent at node A selects any of the parameters and transfers it to R1. If it is a positive reply then it is an authorized node and permitted for deets transformation which is of ciphered form. Ciphering and deciphering is done by AES algorithm. We use Ant-routing scheme to select a relay node. Each node is considered to be an end e-ant. Initially they will be in sleep mode and the pheromone value (Ph) is zero. When data is generated at node A relay node is found in a random manner. Gossiping method is used to measure the productivity of relay node. In this way relay node could be chosen from Ph value and used for broadcasting. Lodis of A-Lodis indicates routing using gossiping technique where nodes can guess the adjacent node location which helps to reach the sink node. Thus secure communication is made possible. Delay in authentication is maintained at its normal level, since these methods use only few seconds to yield the required output. Algorithm for secured A-Lodis and Ant-routing for A-Lodis is shown in **Figure 4**.

5. Simulation Results

Simulated results of A-Lodis with the set of agent with assured security at each node encounter are explained below. The goal is to achieve a secure communication without any loss in regular performance. We use a simulator [20] to examine the protocol. ER (One of the conventional routing scheme) and SNW (with best performance) act as a comparator with A-Lodis with agent AES to highlight its yields. Scenario setup for A-LA is illustrated in section V.A. Performance comparison of A-LA in contrast to ER and SNW are added in section V.B

5.1. Scenario Setup

Parameters compatible for one simulator are listed in **Table 1**.

It uses the pheromone mobility model. The nodes move in an area of 2000 × 2000 m with a speed limit [21] within bounds 0.5 to 1.5 m/s. The radio range is set to 250 m. Total number of nodes within the set network is its node density with which efficiency is determined. Packets are induced with its primary set up of simulation and held over the simulation time. 600s is the average (TTL) or packet life time which subject to change on the performance basis. During examination simulation is run for 3000s.

5.2. Performance of A-LA

Assigning individual agent at each node should no way make any effect in performance of LAROD-LoDis.

```
Ant in sleep mode
    PH = 0;
Generate packet at node A
 Random mode ()
 //node move in random manner in search of another node to deliver the data packet
do
   Relay Ant ()
   //chose the relay node by using gossiping technique
   Trail ()
      PH += 1;
Until destined node is reached
if  Relay Ant is inactive
   for every t == 30 sec
      PH --;
if  PH == 0
   node is ahead of transmission
```

Figure 4. Pseudocode for Ant routing in A-LoDiS.

Table 1. Basic simulation parameters.

Parameters	One Simulator
Area	2000 × 2000 m
Mobility Model	Pheromone
Node Density	200 nodes
Node Speed	1.5 m/s
Radio Range	250 m
Packet Life Time	600 s

Time taken to route packet is directly proportional to the setting of agents which ensures top-level security in ICMANET. In this paper we come up with an apt yield by setting agent at each node. Transmission of data is preceded with ciphering and deciphering of data using AES algorithm. The execution of protocol is evaluated by node speed density, its variation of life time to which the overhead, number of transmissions, delivery ratio and delay are to be maintained favorably. Maximum security is bestowed with the help of agents.

5.3. Performance Comparison of A-LA with ER and SNW

To highlight the benefit of A-LA we analogize it with ER and SNW. Analogy is done with following metrics:

(i) Performance with respect to Delivery Ratio.

(ii) Performance with respect to Malicious Nodes.

To enlighten the secure routing it is estimated with number of node separated from network as well as number of packets routed through them. Regarding mobility and number o nodes in network these are examined.

5.3.1. Performance with Respect to Delivery Ratio

In delivery ratio analysis, A-LA stands to be better than ER and SNW in delivering the message. Evaluation results by modifying the number of nodes and transmission range is shown in **Figure 5** and **Figure 6** respectively. SNW yields maximum delivery when compared to ER and out of these three A-LA is best, because of non-usage of intermediate nodes. Data transmission is done by pair-wise connectivity and node mobility through

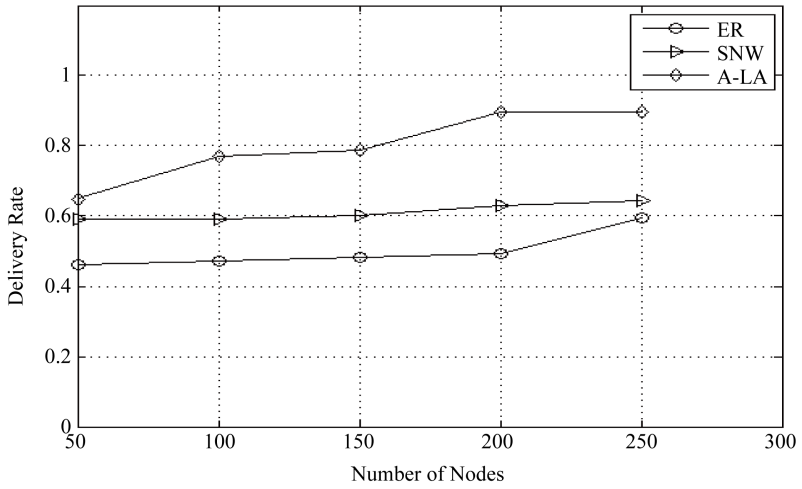

Figure 5. Delivery ratio for various numbers of nodes.

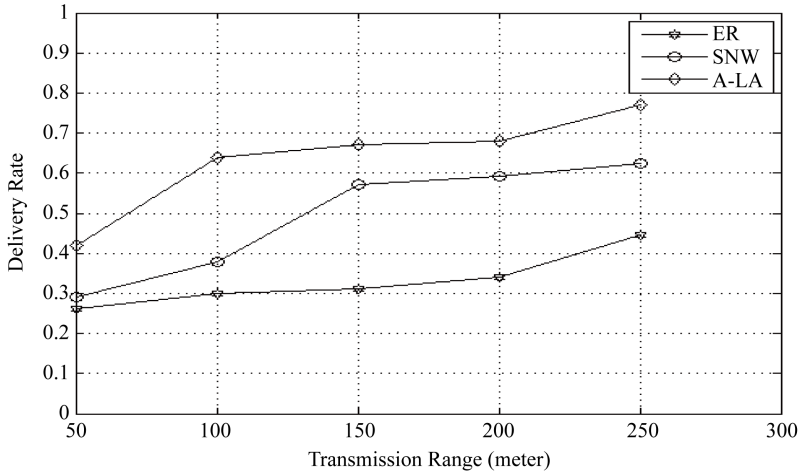

Figure 6. Delivery ratio by varying transmission range.

spraying in ER and SNW respectively which brings variation in probability. A-LA uses the adjacent intermediate node that it encounters during node mobility which makes out to be best among three. Performance variation of their three methodologies is shown in the figure which describes that performance is in no way affected due to authentication.

5.3.2. Performance with Respect to Malicious Nodes

We examine security in reference to isolated nodes and data packets routed through them. The influence of secure routing scheme is evaluated with separated in a network. Due to the usage of authentication, the feasibility of A-LA to detect node in the network is high which is darkened in **Figure 7**. In ER and SNW, this is low as they depend on intermediate node for data transmission. As gossiping process is used for authentication number of nodes in the network is directly proportional to node. Absence of sharing scheme makes the node detection a exigent one in ER and SNW.

Figure 8 shows the probability of routing with malicious node is less in A-LA than in ER and SNW, which is present in A-LA.

It is crystal clear that A-LA is efficient for secure routing in ICMN. The A-Lodis is capable of conquering attacks described below.

(i) **Dropping Data Packets:** this denial of service attack is detected as the malicious nodes do not answer the query posed by agent at each node.

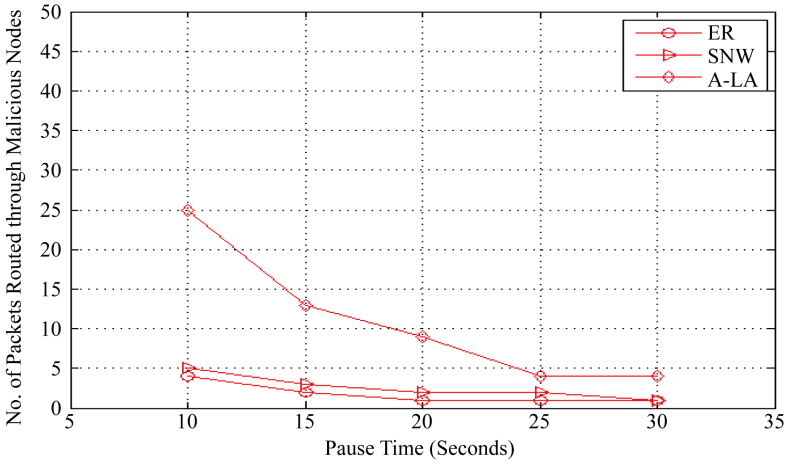

Figure 7. Number of malicious nodes isolated with respect to mobility.

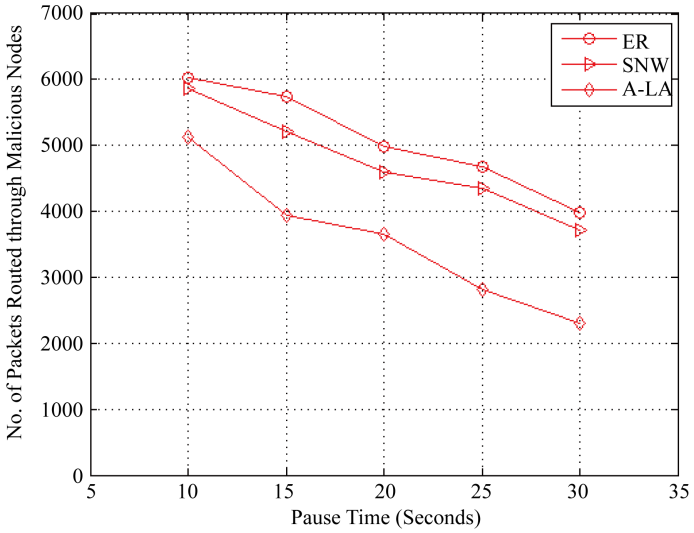

Figure 8. Number of packets routed through malicious nodes with respect to mobility.

(ii) **Dropping Control Packets:** this denial of service attack is detected as the malicious node does not route the data packet as it fails to answer the query generated by agent at each node.

(iii) **Flooding:** This fails since each node detects its adjacent node for data transmission.

(iv) **Gray hole:** as agent queries and information regarding the relay nodes are updated within regular intervals, this attack will be detected.

(v) **Spoofing:** As same answer can't be generated twice during the answer verification scheme, spoofing is detected.

6. Conclusion

Secure data transmission is made possible in this paper. Agent technology ensures the authorization terms at each node. Agent parameters assist to detect the node and security is invoked with AES algorithm. Even after introducing these schemes, the ordinary performance of routing is not eradicated. Delivery rate, minimum delay and constant overhead are same in A-LA and LLR. A-LA is highlighted with scalable security. Presence of agent promises for secure data communication; whose presence is a key to detect the node. The basic properties of LLR protocol like fewer transmission, low contention, better delivery delay and high scalability are attained with generalized value. A comparative analysis and its corresponding results are enlightened in this paper.

Without eradicating the performance, secure communication is made possible. This paper demonstrates secure routing with agent technology and cryptographic mechanisms and is tested with the malicious nodes.

References

[1] Stamouli, I., Argyroudis, P.G. and Tewari, H. (2005) Real-Time Intrusion Detection for Ad Hoc Networks. *IEEE* 6*th International Symposium on a World of Wireless Mobile and Multimedia Networks*, Taormina, 13-16 June 2005, 374-380.

[2] Cokuslu, D. and Erciyes, K. (2008) A Flooding Based Routing Algorithm for Mobile Ad Hoc Networks. *IEEE* 16*th. International Conference on Signal Processing, Communication and Applications*, Aydin, 20-22 April 2008, 1-5.

[3] Vahdat, A. and Becker, D. (2000) Epidemic Routing for Partially Connected Ad Hoc Networks. Duke Univ., Duhram, NC, TecH.Rep. CS-2000-06.

[4] Heissenbüttel, M., Braun, T., Bernoulli, T. and Wälchi, M. (2004) BLR: Beaconless Routing Algorithm for Mobile Ad Hoc Networks. *Computer Communications*, **27**, 1076-1088. http://dx.doi.org/10.1016/j.comcom.2004.01.012

[5] Musolesi, M., Hailes, S. and Mascolo, C. (2005) Adaptive Routing for Intermittently Connected Mobile Ad Hoc Networks. *IEEE* 6*th International Symposium on a World of Wireless Mobile and Multimedia Networks*, Taormina, 13-16 June 2005, 183-189.

[6] Choudhury, R.R. (2005) Brownian Gossip: Exploiting Node Mobility to Diffuse Information in Ad Hoc Networks. *2005 International Conference on Collaborative Computing: Networking, Applications and Worksharing*, San Jose. http://dx.doi.org/10.1109/colcom.2005.1651262

[7] Ghosh, J., Westphal, C., Ngo, H. and Qiao, C. (2006) Bridging Intermittently Connected Mobile Ad Hoc Networks (ICMAN) with Sociological Orbits. *IEEE* 25*th International Conference on Computer Communications*, Barcelona, 23-29 April 2006, 1-3.

[8] Li, Z. and Shen, H. (2008) A Direction Based Geographic Routing Scheme for Intermittently Connected Mobile Networks. *IEEE/IFIP Int., Conf.,Embedded and Ubiquitous Computing*, Shanghai, 17-20 December 2008, 359-365.

[9] Spyropoulos, T., Psounis, K. and Ragavendra, C.S. (2008) Efficient Routing in Intermittently Connected Mobile Networks: The Single-Copy Case. *IEEE/ACM Transactions on Networking*, **16**, 63-76. http://dx.doi.org/10.1109/TNET.2007.897962

[10] Spyropoulos, T., Psounis, K. and Ragavendra, C. (2008) Efficient Routing in Intermittently Connected Mobile Networks: The Multiple-Copy Case. *IEEE/ACM Transactions on Networking*, **16**, 77-90. http://dx.doi.org/10.1109/TNET.2007.897964

[11] Shi, K. (2010) Semi-Probablistic Routing in Intermittently Connected Mobile Ad-Hoc Networks. *Journal of Information Science and Engineering*, **26**, 1677-1693.

[12] Jebajothi, E.J., Kavitha, V. and Kavitha, T. (2010) Contention Based Routing in Mobile Ad Hoc Networks with Multiple Copies. *International Journal of Engineering and Technology*, **2**, 93-96.

[13] Kuiper, E. and Nadim-Tehrani, S. (2011) Geographical Routing with Location Services in Intermittently Connected MANETs. *IEEE Transactions on Vehicular Technology*, **60**, 592-694. http://dx.doi.org/10.1109/TVT.2010.2091658

[14] Spyropoulos, T., Psounis, K. and Raghavendra, C.S. (2005) Spray and Wait: An Efficient Routing Scheme for Intermittently Connected Mobile Networks. *ACM Special Interest Group on Data Communications Workshop Delay—Tolerant Networking*, Philadelphia, 22-26 August 2005, 252-253.

[15] Lai, W.K., Chung, W.K., Tsai, J.B. and Shieh, C.S. (2009) Spray and Hop: Efficient Utility-Mobility Routing for Intermittently Connected Mobile Networks. *IEEE* 4*th International Conference on Communications and Networking*, Location, Xian, 26-28 August 2009, 1-5.

[16] Song, X., Li, B. and Yang, H. (2006) Improved Ant Colony Algorithm and Its Applications in TSP. *IEEE Proceedings of* 6*th Inter. Conf. on Intelligent Systems design and Applications* (*ISDA*'06), Jinan, 16-18 October 2006, 1145-1148.

[17] Ioannis, K., Dimitriou, T. and Freiling, F.C. (1997) Towards Intrusion Detection in Wireless Sensor Networks. 13*th European Wireless Conference*, Paris, 1-4 April 2007, 1-10.

[18] Sekaran, R. and Parasuraman, G.K. (2014) A Secure 3-Way Routing Protocol for Intermittently Connected Mobile Adhoc Networks. *The Scientific Journal*, **2014**, Article ID: 865071. http://dx.doi.org/10.1155/2014/865071

[19] Mow, W. (2006) Modern Cryptography, Theory and Practice. 4th Edition, Pearson Education, New Delhi, 1-648.

[20] Keranen, A., Ott, J. and Karkkainen, T. (2009) The One Simulator for DTN Protocol Evaluation. *International Conference on Simulation Tools and Techniques*, Rome, 2-4 March 2009, 1-10.

[21] Keranen, A. (2008) Opportunistic Network Environment Simulator. *Special Assignment Report, Helsinki University of Technology, Department of Communications and Networking*, Finland.