International Journal of Future Generation Communication and Networking
Vol. 13, No. 3, (2020), pp. 201 - 207

Stable and Secured Multicast Routing (SSMR) in Mobile Ad Hoc Network

[1]P. Vigneshwaran*
[2]M Sindhuja*
[1]*Professor, Department of Computer Science and Engineering, Faculty of Engineering & Technology, Jain University, Bangalore – 562 112*
[2]*Assistant Professor (SG), Department of Information Technology, Rajalakshmi Engineering College, Chennai – 602 501.*

Abstract

Mobile Ad Hoc Network (MANET) could be assortment of mobile nodes connected along and changes its location haphazardly. Because of this nature, security of the mobile network is extremely less. Any un-trusted party penetrates the knowledge into the network exploitation baptized malicious attack. A stable and secure algorithm is obligatory to spot and take away the malicious nodes to boost the network performance. The Stable and Secured Multicast Routing algorithm (SSMR) is employed to spot the set of disjoint routes thought-about as secure routes that square measure free from malicious attack. Secure routes would square measure known by the trustworthy nodes that schemes the values of knowledge augmented in the packet. The SSMR has identified the set of disjoint secure nodes to construct the secure path for transmission. This action reduces the packet loss to massive extent and successively improves the packet delivery proportion by ninety eight. SSMR has speckled the set of disjoint routes as secure routes which are liberated as of malicious nodes. Also, the occurrence of a malicious node inside the set-up causes packet loss throughout the transmission. SSMR is achieved ninety eight of packet delivery ratio with reduced overhead in the network.
Keywords: *Mobile, Packet loss, Routing, Stable, Security.*

1. Introduction

The effective communication of an organization determines it success. Mobile Ad hoc Networks (MANET) will improve the communication significantly by providing connectivity to the nodes from everyplace at anytime. MANET has seen and deployed in many applications related to commercial and non-commercial areas. In all those areas security aspect is on the more focus. MANET is insecure in nature and it is more vulnerable than wired networks. This is mainly because of the free will among the nodes in the direction of joining a network or to move anywhere within the network or to disappear a network. Compromised nodes exhibiting malicious behaviors are tough just before detect; as soon as there is a need to contain such a centralized coordinator it will be short of centralized machinery might also purpose problems; restricted energy supply can cause some problems, and continually changing the size of the network have identified with better requirement to improve the working of the protocols and services in MANET. As a result, in contrast with the wired network, MANET will need more robust schemes to ensure its security. There are few of the reasons for challenges in security in MANET:

- The wireless networks especially are liable to attacks because of active eavesdropping to passive interfering.
- Lack of Trusted Third Party (TTP)
- Limited computation capability
- Power consumption functionalities
- Infrastructure less and self-organizing property.
- Hard to discriminate stale routing and replicated routing data due to the fact of node mobility mechanism. In the node mobility mechanism, it enforces widely wide-spread networking reconfiguration which creates greater probabilities for attacks.

Several security mechanisms have been implemented to counteract malicious attacks in MANET. Among those the first line of defense was usually given by authentication, access control, encryption, and digital signature. IDS and Cooperation enforcement mechanisms act as second line of defense. Furthermore facilitate to defend in opposition to enforce cooperation or attacks, dropping selfish node behaviour. Proposed solutions on Multicast security issues includes been studied in a number of works (Moyer et al 1999; Cannetti et al 1999).

The major targets of multicast protection communications are to preserve confidentiality and assurance

ISSN: 2233-7857 IJFGCN

authentication intended for all crew message; so with the intention of only reputable sender be able to multicast packets towards the group and solely packets dispatched by using professional team individuals are accepted. To shield the community from clogging attacks multicast safety presents offerings towards anonymity, non-repudiation, get entry to manage issues, and have confidence issues. Security in multicast is consequently regarded greater difficult than in the unicast operation. Factors affecting protection are team size, group type, member (node) characteristics, membership dynamics, wide assortment and sort of senders, volume and kind of traffic and directing calculation utilized. Hence, multicast security is a genuinely confounded multi-faceted, multi-layered issue. Those necessities are even extra hard to satisfy in advert hoc systems the spot transmission capacity, stockpiling, and power requirements of the hubs represent extra issues when combined with versatility and progressively adjusting topology without an incorporated foundation. MANET brings new security difficulties to arrange structure because of this nature. MANET is more powerless against assaults than wired systems or infrastructure based wireless networks. Security has the primary goal to provide confined communication between nodes.

2. Related Works

Yu et al [1] proposed a dispensed hierarchical key management scheme which accepted as true with would be properly desirable for calculated MANETs. The methods can dynamically choice of fine nodes towards work as the Private Key Generator (PKG) to enhance MANET safety and maximize the community lifetime. Ning Jiang et al [2] proposed a novel strategy to enforcing collaboration and security in cellular networks. The nodes preserve local recognition of their neighbor nodes through direct surveillance. Erman Ayday et al [3] Delay Tolerant Networks (DTN) proposed an efficient, robust trust mechanism and low cost malicious node detection technique. Feng li et al [4] proposed a dynamic Bayesian game framework for analyzing the wrestle between regular and compromised nodes. Balasubramanian et al [5] proposed a dynamic Bayesian signaling model to identify mis-behavior nodes using stranger target interactions in MANETs. Shengrong Bu et al [6] offered a distributed method via merging substantiation and infringement detection systems. Tang et al [7] offered a bio-inspired consensus to contradict SSDF attacks in Cognitive Radio. The proposed scheme differentiates the reliability of variety sensing terminal, which makes it vigorous adjacent to Spectrum Sensing Data Falsification attacks. Yi Ping et al [8] proposed an intrusion detection system based on timed automata that facilitate to detect attacks on the Dynamic Source Routing protocol. Serique et al [9] proposed a mechanism that aims to ease the misbehavior in routing and other network failures. Shakshuki et al [10] proposed an Enhanced Adaptive Acknowledgment (EAACK) protocol particularly designed in favor of MANETs. The proposed system is solved to deal with 3 of the 6 weakness of Watchdog method, that is, restricted transmission power, false misbehavior, and receiver collision. Gaeta et al [11] proposed the novel disbursed technique SIEVE to identify the malicious nodes by performing air pollution attack in the MANET. Kurt Derr et al [12] proposed an algorithm named as Extended Virtual Spring Mesh (EVSM). The proposed algorithm has verified to be an positive allotted self-organizing algorithm for deploying a MANET in an area with obstacles. Gaeta et al [13] proposed Belief Propagation method to compute the probabilities of peers who are being misbehave. Whenever the network receives a chunk of data from the peers the algorithm is executed by the monitor node.

Eduardo Da Silva et al [14] presented an identity-based key management technique in which the private key of users must be known by the key management authority. Marchang et al [15] presented a light-weight trust-based routing protocol. The routing alogorithm is executed by every node in the network independently, and it used only local information to maintain the scalability. Ruj Akavipat et al [16] presented a reputation-based mechanism for improving the flexibility of searches in Halo and Kad, against misbehavior nodes. Zhang et al [17] prposed a secure, lightweight, scalable Identity -based Key Management (IKM) scheme that permits the common keys of mobile nodes to be directly computable from their known network IDs. Li et al [18] proposed a fully-distributed Identity based multiple secrets Key Management scheme (IMKM). The proposed system is implemented through a mixture of Identity based multiple secrets and techniques and threshold cryptography. Yanchao Shengrong Bu et al [19] proposed a disbursed scheme which is the combination of user authentication and intrusion detection. Li et al [20] incorporated the idea of have confidence to MANETs and construct a simple believe mannequin to consider neighbors' behaviors – forwarding packets. Xia et al [21] proposed a novel have faith management mannequin that uses AHP concept and good judgment regulations prediction technique which is used to consider to have the confidence of nodes. Soonhwa Sung et al [22] proposed zone based self organized clustering broadcast technique that is capable of converse securely smooth if the nation changeover of nodes is threatened by corrupted nodes.

ISSN: 2233-7857 IJFGCN

Based on top of the related works it is found that many routing protocols have been designed to identify secure nodes and secure routes among the nodes in the network, but still there is performance degradation during the malicious attack. One of the reasons for the performance degradation is the active involvement of the misbehavior nodes in the environment. Anomaly nodes in the network spread the fake route notifications and perform the replay attack in the network. Any malicious nodes in the network still disturb the whole process or even stop the entire process by intercepting the regular activities of the node. The following attacks are possible when a node breaks the security principles. They are packet dropping rate and injecting the duplicate packets , battery drain, buffer overflow, bandwidth consumption, malicious node, stale routes and packets, delay, link break, message tampering, impersonation, Denial of Service (DoS), and session capturing. If the malicious nodes enter into the network, it injects the unwanted packet and increases the overhead to the network. These attacks lead to the severe performance degradation in terms of PDR, network life time, delay and bandwidth utilization. It is clearly stated that to devise an algorithm to strengthen the security of the multicast routing protocols to overcome the malicious node attacks such as tampering, impersonation and replay attacks. The proposed algorithm will enhance the security service for the message communication such as confidentiality and authentication.

3. Identification of Malicious Node

The proposed system deals with the generation of stable and secure routes in the network. Identifying and avoiding the malicious nodes may reduce the number of packets dropped. Therefore finding the secure routes to transfer the encrypted message requires a secret key. The proposed systems used a Shamir's Secret Sharing (SS) scheme to generate a secret key and divides the secret key into n number of shares (or secrets) based on the number of available routes. This is used to identify all secure routes successfully and the secure nodes are identified with additional information augmented in the JOIN_QUERY such as Link duration (LD), Energy (E), Mobility Speed (MS), and Route Refresh time (RRT). Amongst all the secure nodes, secure routes are identified by applying SS. The secure and final routes are determined with the average value of the additional information augmented in the route request packet. The secure routes are identified by the average value of MS, E, LD & RRT. The threshold has been fixed for these values to identify the stable nodes for message transmission. If any node is having higher value than the threshold and those nodes are identified as stable nodes. With the help of the nodes the stable and secure routes are constructed using SS principle. The messages are transmitted only with the secure routes. The route maintenance phase is established to identify the new routes, if any node leaves the network.

4. Identification of Secure Routes

Secure routes can be detected by using Secret Key (SK). Source node divides the secret key SKs into n shares, the place n = quantity of routes accessible commencing from source to destination pairs. At this time supply node generate F(x) based on Equation 1.

$$F(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_{k-1} x^{k-1} \quad (1)$$

Where 'a' is set of integers

'n' quantity of factors as of polynomial which will be P1, P2, P3 etc., generated by utilizing source node and sends each of these factors in encrypted structure thru each amongst n unique reachable routes. These 'n' points are decrypted by the destination node and again encrypt these factors and routes to the source node through backtracking by using the reverse path which it is received. Source is encrypted using these 'n' factors and takes the suitable nearest point amongst them to regenerate the polynomial $F_1(x)$ the usage of Lagrange's Interpolation in Equation (2).

$$F_1(x) = \sum_{r=0}^{k-1} Y_r \prod_{i=0, i \neq r}^{k-1} \frac{x - x_i}{x_r - x_i} \quad (2)$$

The first consistent section of $F_1(x)$ is called SK_1. If SKs = SK_1, these factors are legitimate points that are used to find the secure routes.

5. Results and Discussion

Table 1 shows the simulation environment. In our simulation, in which NS2 is used with the channel

ISSN: 2233-7857 IJFGCN

capability of cell hosts is set to 2 Mbps. The dispensed coordination characteristic is used to get notified about the link breakage. Mobile nodes cross in a one thousand meter x one thousand meter rectangular location for 400 seconds simulation time. With the random waypoint (RWP) model from NS2, initial areas and actions of the nodes are obtained. Each node strikes independently with average speed (20m/s) and all the nodes have identical transmission vary around 250 m.

Table 1 Simulation Setup in NS2

Area	1000 m X 1000 m
MAC Protocol	IEEE 802.11 DCF
Wireless Channel	Free Space Propagation Model
Number of Nodes	10, 20, 30, 40, 50
Traffic Type	Constant Bit Rate
Mobility Model	Random way point
Mobility Speed	20 m/s
Radio Range	250 m
Simulation Time	400 ms
Pause Time	0 Sec
Initial Energy of the Node	1500 Joules
Packet Size	Default size (512 Bytes)
Channel Capacity	2 Mbps
Route Refresh Time	5 Seconds

A node randomly selects a destination from all the physical terrain in this particular mobility model. It strikes with uniform speed in all the sides of the destination. The node strikes again after a stay there with a pause time when it reaches its destination,. In this simulation, the maximal velocity is set as 10 m/s. and interval time is set as 0 sec. It is simulated to range the range of nodes as 5, 10, 15, 20, 25, 30, 35, 40, 45 and 50, to look at the overall performance have an impact on of one-of-a-kind topologies. Constant Bit Rate (CBR) traffic is simulated here. For every scenario, the received results were averaged by 10 runs with random seeds carried out. The algorithm is in contrast with traditional systems based on the broad range of network traits such as packet dropped, PDR, cease -to-end delay and overhead. The keys are securely transmitted and the secure routes are recognized primarily based on the node's have confidence value. Figure 1 shows the formation of network and identification of malicious node during the transmission of data. Source, Receivers and malicious nodes are clearly represented with different colors. The nodes represented by yellow colors are malicious node. Due to the malicious node behaviour, the packets are dropped at the receiving end.

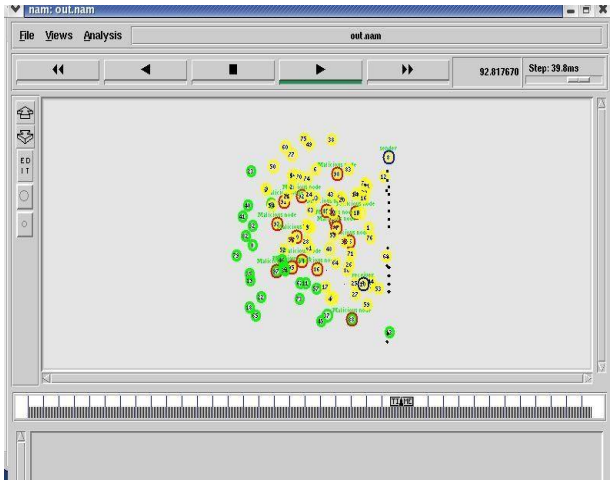

Figure1. Malicious node detection

ISSN: 2233-7857 IJFGCN

In Figure 2 shows the packet delivery rate of nodes is compared with other secure multicast routing. The proposed algorithm produces more than 95% of packet delivery due to the nature of encryption and decryption methods. The messages are transmitted to the multicast receivers with the help of secure routes identified by the secret sharing scheme. Secure routes are identified by trustworthy nodes in the network. The computation time of this algorithm is less compared to other conventional systems. Due to this nature of the proposed algorithm, it achieves a higher PDR compared to other conventional systems such as SCAN, SEAD and Ariadne.

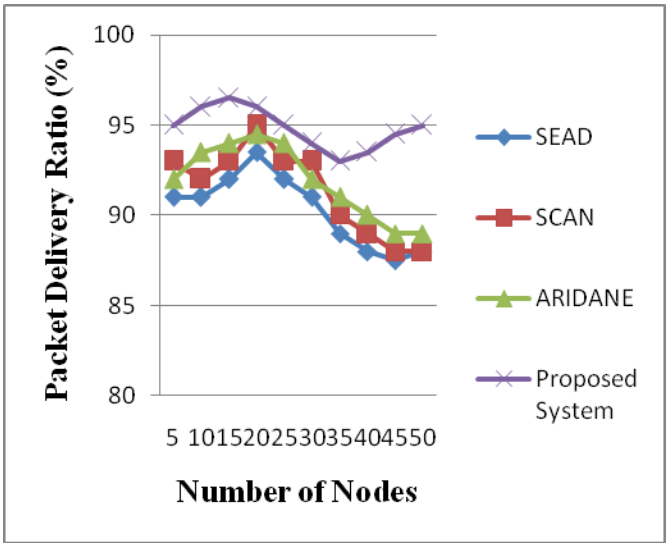

Figure 2. Number of Nodes Vs Packet Delivery Ratio

Figure 3 shows the packet loss of the proposed algorithm with other secure multicast routing. It produces less packet loss, since the entire message is encrypted, hash values are calculated for the message and it is transmitted to the multicast receivers. Any intermediate nodes are not able to recover the message without having the knowledge of the key and algorithm. But, packet loss increases when number of nodes also increases.

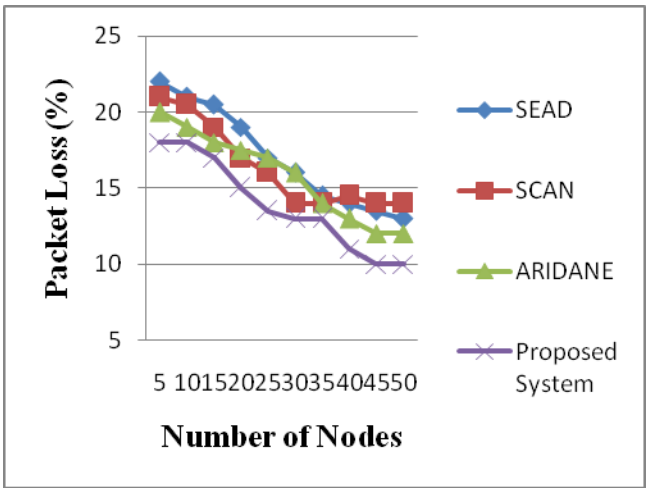

Figure 3. Number of Nodes Vs Packet Loss

The reduction in packet loss is due to the identification of malicious nodes and thereby creating a stable and secure route between the source and destination. The sender circumvents potentially malicious nodes, and enables it to authenticate every node in a route discovery process.

6. Conclusion

Securing MANET is a very challenging issue. Malicious nodes in the community will end result in high packet loss and excessive manipulate overhead. The impenetrable and Stable Multicast Routing Algorithm (SSMR) tried to perceive disjoint routes viewed as impenetrable paths which is free from the anomaly nodes. This minimizes the packet drop ratio and also detects all secure routes. Along with balance and trust value, mobility of

ISSN: 2233-7857 IJFGCN

the node becomes an essential factor for selecting a steady and a robust route. To reap the stability the relied on nodes are identified based on the common price of the extra facts augmented in the JOIN_QUERY packet. The key energy of this algorithm is that the routes are identified with the aid of the honest nodes based totally on the calculated values of statistics augmented in the JOIN_QUERY. The algorithm used the Secret Sharing to devise the secure routes among the networks. The presence of malicious node in a network causes packet loss in the course of the transmission of messages via that node. The secure and secured multicast routing attempts to discover the set of disjoint impervious nodes viewed as secure routes. This action as a consequence reduces the packet loss in the large extent and in flip improves the packet shipping ratio.

References

[1] G F. Richard Yu, Helen Tang, Peter C. Mason, Fei Wang, "A Hierarchical Identity Based Key Management Scheme in Tactical Mobile Ad Hoc Networks", IEEE Transactions on Network and Service Management, vol7, no.4, DECEMBER 2010, pp. 258-267.

[2] Ning Jiang, Kien A. Hua, Danzhou Liu, "A Scalable and Robust Approach to Collaboration Enforcement in Mobile Ad-Hoc Networks", Journala of Communications and Networks, vol.9, no.1, MARCH 2007, pp. 56-66.

[3] Erman Ayday, Faramarz Fekri, "An Iterative Algorithm for Trust Management and Adversary Detection for Delay-Tolerant Networks", IEEE Transactions on Mobile Computing, vol.11, no. 9, SEPTEMBER 2012, pp.1514-1531.

[4] Feng Li, Yinying Yang, Jie Wu, "Attack and Flee: Game-Theory-Based Analysis on Interactions among Nodes in MANETs", IEEE Transactions on Systems, Man, and Cybernetics—Part B: Cybernetics, vol.40, no.3, JUNE 2010, pp.612-622.

[5] Balasubramanian Paramasivan, Maria Johan Viju Prakash, Madasamy Kaliappan, "Development of a Secure Routing Protocol using Game Theory Model in Mobile Ad Hoc Networks", Journal of Communications And Networks, vol.17, no.1, FEBRUARY 2015, pp.75-83.

[6] Shengrong Bu, F. Richard Yu, Xiaoping P. Liu, Peter Mason, Helen Tang," Distributed Combined Authentication and Intrusion Detection with Data Fusion in High-Security Mobile Ad Hoc Networks", IEEE Transactions on Vehicular technology, vol.60, no.3, MARCH 2011, pp.1025-1036.

[7] H. Tang, F.R. Yu, M. Huang, Z. Li, "Distributed consensus-based security mechanisms in cognitive radio mobile ad hoc networks", IET Communication, 2012, vol.6, no.8, pp.974–983.

[8] Yi Ping, Jiang Xinghao, Wu Yue & Liu Ning, "Distributed intrusion detection for mobile ad hoc networks", Journal of Systems Engineering and Electronics, vol.19, no.4, 2008, pp.851–859.

[9] L. F. S. Serique Junior and R. T. de Sousa Junior, "Evaluating Trust in Ad Hoc Network Routing by Induction of Decision Trees", IEEE Latin America Transactions, vol.10, no.1, JAN. 2012, pp.1332-1343.

[10] Elhadi M. Shakshuki, Nan Kang, and Tarek R. Sheltami, "EAACK—A Secure Intrusion-Detection System for MANETs". IEEE Transactions on Industrial Electronics, vol.60, no.3, MARCH 2013, pp.1089-1098.

[11] P Vigneshwaran, R Dhanasekaran, " Optimum Selection of Forwarding Group Node in Multicast Routing Protocols", International Journal of Advancements in Computing Technology, vol. 7, no. 2, March 2015, pp. 60 -71

[12] Rossano Gaeta, Marco Grangetto, Riccardo Loti, "Exploiting Rateless Codes and Belief Propagation to Infer Identity of Polluters in MANET'', IEEE Transactions on Mobile Computing, vol.13, no.7, JULY 2014, pp.1482-1494.

[13] Kurt Derr, Milos Manic, "Extended Virtual Spring Mesh (EVSM): The Distributed Self-Organizing Mobile Ad Hoc Network for Area Exploration", IEEE Transactions on Industrial Electronics, vol.58, no.12, DECEMBER 2011, pp.5424 – 5437.

[14] Rossano Gaeta and Marco Grangetto," Identification of Malicious Nodes in Peer-to-Peer Streaming: A Belief Propagation-Based Technique", IEEE Transactions on Parallel and Distributed Systems, vol.24, no.10, OCTOBER 2013, pp.1994-2003.

[15] Eduardo Da Silva, Aldri L. Dos Santos, Luiz Carlos P. Albini, Michele N. Lima," Identity-Based Key Management in Mobile Ad Hoc Networks: Techniques and Applications", IEEE Wireless Communications, October 2008, pp. 1536-1284.

[16] N. Marchang R. Datta," Light-weight trust-based routing protocol for mobile ad hoc networks", IET Information Security, 2012, vol. 6, no. 2, pp.77–83.

[17] Ruj Akavipat, Mahdi N. Al-Ameen, Apu Kapadia, Zahid Rahman, Roman Schlegel, Matthew Wright, "ReDS: A Framework for Reputation-Enhanced DHTs", IEEE Transactions on Parallel and Distributed Systems, vol.25, no.2, FEBRUARY 2014, pp.321-331.

[18] Yanchao Zhang, Wei Liu, Wenjing Lou, Yuguang Fang, "Securing Mobile Ad Hoc Networks with

ISSN: 2233-7857 IJFGCN

Certificateless Public Keys", IEEE Transactions on Dependable And Secure Computing, vol.3, no.4, OCTOBER-DECEMBER 2006, pp.386-399.

[19] Lung-Chung Li and Ru-Sheng Liu," Securing Cluster-Based Ad Hoc Networks with Distributed Authorities", IEEE Transactions on Wireless Communications, vol.9, no.10, OCTOBER 2010, pp.3072-3081.

[20] Shengrong Bu, F. Richard Yu, Xiaoping P. Liu, Helen Tang," Structural Results for Combined Continuous User Authentication and Intrusion Detection in High Security Mobile Ad-Hoc Networks", IEEE Transactions on Wireless Communications, vol.10, no.9, SEPTEMBER 2011, pp.3064-3073.

[21] X. Li Z. Jia P. Zhang R. Zhang H. Wang, "Trust-based on-demand multipath routing in mobile ad hoc networks", IET Information Security, vol.4, no.4, 2010, pp.212–232.

[22] H. Xia, Z. Jia, L. Ju, Y. Zhu," Trust management model for mobile ad hoc network based on analytic hierarchy process and fuzzy theory", IET Wireless Sensor Systems, vol.1, no.4, 2011, pp.248–266.

[23] Soonhwa Sung, "Zone-Based Self-Organized Clustering with Byzantine Agreement in MANET" , Journal of Communications and Networks, vol.10, no.2, June 2008, pp.221-227.

[24] Mohammad Siraj, Soumen Kanrar "Performance of Modeling wireless networks in Realistic environment" International Journal of Computer Networks, vol.2, no. 1, 2010, pp. 62-79.

[25] Ditipriya Sinha, Uma Bhattacharya, Rituparna Chaki. "RSRP: A Robust Secure Routing Protocol in MANET", Foundations of Computing and Decision Sciences, 2014

[26] Kumari, S. Vadhana, and B. Paramasivan. "Ant based Defense Mechanism for Selective Forwarding Attack in MANET", 2015 31st IEEE International Conference on Data Engineering Workshops, 2015.

ISSN: 2233-7857 IJFGCN