Volume 3, Issue 11, November 2013 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

SMBP: Framework for Surveillance of Malicious Behaviour Pattern in Mobile Adhoc Network

Sumati Ramakrishna Gowda
Research Scholar
Vinayaka Missions University
Salem, India

P.S Hiremath
Professor and Chairman
Department of Computer Science
Gulbarga University Gulbarga, India

Abstract— Understanding the node misbehavior, routing issues, and visualizing the patterns of attacking policies adopted by intruder/malicious node are some of the most challenging tasks in MANET due to its complex inherent security issues that are yet to be effectively addressed. The proposed system introduces a novel technique as a solution to understand in true sense the various uncertain strategies which are computationally most challenging task for visualizing the malicious node and their attack policies. Powered by mechanism design, the proposed framework has addressed various routing issues that surfaces due to the presence of selfish / malicious nodes in mobile adhoc network. In order to evaluate the simulation result, the proposed system is compared with some of the frequently used evolutionary algorithms. The simulation result is assessed with respect to detection of attack in independent routing, intrusion in privacy policies as well as simulation time.

Keywords-component: Design Selfish Node, Malicious Node, MANET Mechanism, Security

I. INTRODUCTION

Mobile ad hoc networks (MANETs) characteristics include a dynamic topology, lack of a centralized authority, and a decentralized architecture [1]. The most urgent needs of MANET performance include power consumption, topology control, and spectrum sharing, all of which are intensified by node mobility. These concerns can be alleviated by an optimal node distribution. Achieving better spatial placement may lead to an improvement in area coverage with reduced sensing overshadows and limited blind spots, as well as to the reduction of power consumption, better spectrum utilization, and the simplification of routing procedures. However, the lack of a central omniscient authority controlling all the nodes and limited coordination, typical for medium to large ad hoc networks, may result in a degradation of overall network performance due to the selfishly determined relocations by individual agents. Additional concerns are related to the unknown geographical territory and the hostile environment in which the network may have to operate. Routing is one of the most important services in the network; therefore it is also one of the main targets to which attackers conduct their malicious behaviors. In the mobile ad hoc networks, attacks against routing are generally classified into two categories: attacks on routing protocols and attacks on packet forwarding/delivery [2]. Attacks on routing protocols aim to block the propagation of the routing information to the victim even if there are some routes from the victim to other destinations. Attacks on packet forwarding try to disturb the packet delivery along a predefined path. Because of the mobility and constantly changing topology of the mobile ad hoc networks, it is very difficult to validate all the route messages. There are some more sophisticated routing attacks, which include Wormhole attacks, Rushing attacks and Sybil attacks [3]. The second category of attacks against routing is attacks on packet forwarding/delivery, which are not easy to detect and prevent. There are two main attack strategies in this type: one is selfishness, in which the malicious node selectively drops route messages that are assumed to forward in order to save its own battery power; the other is denial-of-service, in which the adversary sends out overwhelming network traffic to the victim to exhaust its battery power. There are numerous kinds of attacks against the routing layer in the mobile ad hoc networks, some of which are more sophisticated and harder to detect than others, such as Wormhole attacks and Rush attacks. The attacks in MANET can roughly be classified into two major categories, namely passive attacks and active attacks, according to the attack means. A passive attack obtains data exchanged in the network without disrupting the operation of the communications, while an active attack involves information interruption, modification, or fabrication, thereby disrupting the normal functionality of a MANET. The attacks can also be classified into two categories, namely external attacks and internal attacks, according the domain of the attacks. Attacks can also be classified according to network protocol stacks. There are malicious routing attacks that target the routing discovery or maintenance phase by not following the specifications of the routing protocols. Routing message flooding attacks, such as hello flooding, RREQ flooding, acknowledgement flooding, routing table overflow, routing cache poisoning, and routing loop are simple examples of routing attacks targeting the route discovery phase. Proactive routing algorithms, such as DSDV and OLSR, attempt to discover routing information before it is needed, while reactive algorithms, such as DSR and AODV, create routes only when they are needed. Thus, proactive algorithms are more vulnerable to routing table overflow attacks. Related work is

discussed in Section 2 followed by problem description in Section 3. Section 4 highlights the proposed technique followed by implementation and result in Section 5. Finally conclusion summary is given in Section 6.

II. RELATED WORK

This section contains a brief survey of the prior research work done in the area of security system in mobile adhoc network that pertains to the misbehavior problems of the mobile nodes. An extensive study has been done over routing attacks in Mobile Adhoc Network [4-6] where majority of the intruding factors are blackhole, fabrications, and corrupting the structure of the routing data frame. The work done in [7] and [8] however address certain solution against routing attacks in MANET, but the existing studies still do not have answer for efficient security technique that has promising results in safeguarding the communication in MANET. Some of the existing works in the area of providing an efficient security mechanism for MANET are shown in the Table 1.

Table 1 Comparison Chart

Author	Problem Focused	Technique Used
Mishra [9]	Routing Misbehavior	Enhanced Security based on on-demand protocols
Dasgupta [10]	-Routing Misbehavior -Rushing attack on AODV	Designed RREQ forwarding mechanism
Karjee[11]	Routing Misbehavior/attack	Signal bandwidth
Crepeau [12]	Physical security measures	RSR- on demand routing protocol
Li[13]	Security Protocol	Secure Clustering scheme
Li [14]	Issues in Trust management	Multidimensional trustworthy framework
Gong et al. [15]	Incentive mechanism	Security system based on Trust
Orallo et al. [16]	Issues in Node Cooperation schemes	Integrated security system
Manchikalapudi [17]	Issues in Trust management	Evidential Protocol based on trust factor of nodes
Beghriche [18]	Routing Issues and its impact on node behavior	Bayesian Framework

Majority of the above mentioned works are focused on introducing a strong security system that addresses routing behavior or any factors that directly influence node misbehavior. However, these works have used cryptographic approach which always has some or other security loopholes when it comes to wireless networking. It was also found that game theory has a valuable contribution in security of MANET [19], where various approaches are used to mitigate attacks or any malicious activities in MANET. The proposed research work is inspired from all the above mentioned prior studies that mainly motivate to design a stable theoretic framework for analyzing the strategy profiles for both normal and attacker nodes. The evaluation of the pattern of malicious node is done based on decision factors to conclude whether the node is malicious or regular node. However, majority of the evaluation is performed using single attacker. Hence, it is also required to evaluate the impact of multiple attackers on the network security in MANET using game theory. Also, some of the efficient techniques found till date are i) Cooperative security system using shapley value technique, ii) Host based security system using basic signaling game, iii) Leader security system using cooperative game approach, iv) Security system using non cooperative game model, and v) Security system employing Bayesian game approach [20]. However, it was noted in survey work in [20] that there exists severe limitation on almost every approach e.g. i) high processing time, ii) inaccurate response time, iii) selfish node is not considered, iv) alliance of different malicious nodes is not considered, v) small scale network consideration, and vi) less energy efficient that cause higher node death. Hence, the proposed system will target to explore much more better and efficient technique in game theory that addresses the issues of node misbehavior in large scale MANET system and other limitations that were not considered in prior work as mentioned in [19].

III. PROBLEM STATEMENT

The problem descriptions of the proposed system are as follows:

- Selfish Nodes [21] are active in route discovery, but not in packet forwarding. They tend to drop data packets of others to save their energy so that they could transmit more of their own packets and also to reduce the latency of their packets. This type of attack comes under denial-of-service (DoS) category.
- Behavior of selfish nodes, on the other hand, which cooperate during route discovery and defect during packet forwarding, need to be explored. A behavioral model that could dynamically predict the level of cooperation

extended by the node towards the network functions such as routing, network monitoring and packet forwarding is therefore, crucial.

- The common objective of malicious nodes [22] is maximizing the damage to the network while avoiding being caught. Their activities tend to disrupt the operation of the network and waste the resources of regular nodes.

Moreover, malicious nodes have the strategy of escaping detection to avoid punishment in MANETs. Therefore, a malicious node can start its malicious behavior all over again with a clean history in a new location by escaping before being caught. However, this additional strategy does not imply that malicious nodes should continuously attack and run since escape is also associated with a cost (e.g., the energy spent to move to the selected destination). Different types of misbehavior out of different purposes have been created by the misbehaving nodes in an ad hoc network. The types of misbehavior on data related to the work are given below:

- Data Dropping: This is the denial of service (DoS) attack. In this attack, the selfish or malicious intermediate nodes decline to forward data packets for other nodes in the network. In this paper two adverse environments are examined. They represent the types of data dropping misbehavior formed by individual and cooperating misbehaving nodes respectively.
- Individual dropping: This is a relatively simple type of misbehavior. The misbehaving nodes drop all or a certain percent of the received data packets because of unlike intentions. Most schemes [23], [24], [25] detecting misbehavior on data are designed to deal with this kind of misbehavior.
- Colluded dropping: This is an advanced type of misbehavior formed by two cooperating malicious nodes. It is difficult to detect and defend this attack. It is assumed that two malicious intermediate nodes N1 and N2 are connected on a data transmission path. N1 forwards received data packets to N2, and N2 drops all or part of them. N1 tries to cover the data droppings at N2 by ignoring it and/or generating / forwarding faked acknowledgements in the system. As N1 would not report the misbehavior of N2 to the system, the overhearing schemes [26] fail to detect such colluded misbehavior. Since N1 could forward faked 2ACK generated by N2 or generate faked 2ACK for N2, neither of the protocols proposed in [26] could detect such fabricated packets and thus the colluded dropping. The schemes discussed in [27], [28] tackle such colluded misbehavior
- Data Modifying: During data transmission, the malicious nodes alter the received data packets. One malicious node is assumed to form the data modifying misbehavior independently along the data transmission path. Whereas the schemes in [27-28] can successfully detect such misbehavior, the schemes in prior studies cannot detect such kind of misbehavior.

The problem statement of the proposed study is as follows: It is highly computationally challenging task to design a mathematical model for exhibit an extremely unpredictable malicious behavior of the malicious mobile nodes in multiples under diverse vulnerable security conditions in MANET and thereby making it difficult to design a decision making model for ensuring mitigating of attack events and deporting mechanism. A malicious node can easily furnish false information at the time of route discovery process initiated by other regular nodes; they choose to participate even in data packet forwarding in the preliminary phases. This deceptive act of malicious mobile node will eventually gain the trust and belief system of the network where the malicious node wait for an optimal opportunity to initiate a brutal attack on the network. It is to be noted that once the malicious node gains the trust, the more is the intensity of the attack that potentially causes damage to various resources in MANET system. One of the most critical issues of such phenomenon is the identification of behavior of different types of nodes. Eventually, using cryptography or any other techniques, one can stop and mitigate such attacks but cannot solve if the attacking strategy is changed by malicious nodes. Hence, working on intrusion detection system or detecting a malicious node will broaden the scope of study and optimal results on security on large scale MANET cannot be accomplished. Hence, the current research work chooses to simulate the decisions adopted by various types of nodes using game-theory that gives a better statistical probability of equilibrium stages.

IV. PROPOSED SYSTEM

The proposed study is primarily concentrated on addressing the significant security loopholes observed in MANET by studying the malicious behaviour of nodes in simulation environment using random mobility model. The study is conducted by understanding various QoS and security flaws with malicious node avoidance from communication channel. The research is then extended to represent a mathematical model for node misbehavior using potential capabilities of mechanism design [29] in order to differentiate the behaviour between regular and malicious node. Finally, an efficient model termed as Surveillance of Malicious Behaviour Pattern (SMBP) in mobile adhoc network is designed which has the capability of addressing majority of the threats in MANET. The system uses a dynamic mechanism for design modeling to evaluate the communication pattern between regular and malicious nodes in mobile adhoc networks. The proposed SMBP framework will furnish solutions to various security threats by malicious and selfish nodes. The SMBP is designed with defined sets of regular and malicious nodes, which will be distributed randomly. The design constituents in the network will be mobile in nature to assess the behavior of both regular as well as malicious nodes. The application will understand the strategy employed by the malicious node and, finally this information will be used by the regular node for restricting the escape strategy of malicious node to another logical region. In order to report the regular node and malicious nodes that invoke an attack, which comply with the sequential rationality requirement, the proposed SMBP framework will highlight the extensive and smart use of decision rules for regular nodes. The design of SMBP will also study the equilibrium strategy profiles for both regular as well as malicious nodes based on the trust factor and expected payoff and reveal the connection between nodes' best response and the cost

and gain of each individual strategy. Finally, the proposed work will also present a mitigation technique to circumvent the attack consequences. However, the SMBP framework is designed for actually evaluating and sequential mapping of the malicious inflicted mobile nodes and their all possible strategies of attack in any given scenario of MANET application. This will basically exhibit all the topological issues in routing strategy adopted by the transmitting mobile node for data packet forwarding. The prime focus of the SMBP framework design is to permit the communication to initiate among the regular nodes, monitor for all the uneven activities along with all the gain in trust factor for each and every mobile nodes. Any uncharacteristic gain in trust will put that particular node into surveillance. The proposed system will then estimate the uncertainty in opinion adopted by the node. The strategy for the proposed system is depicted in the Fig.1 with the main purpose being surveying all the unpredicted malicious activities from the vulnerable situation in mobile adhoc network.

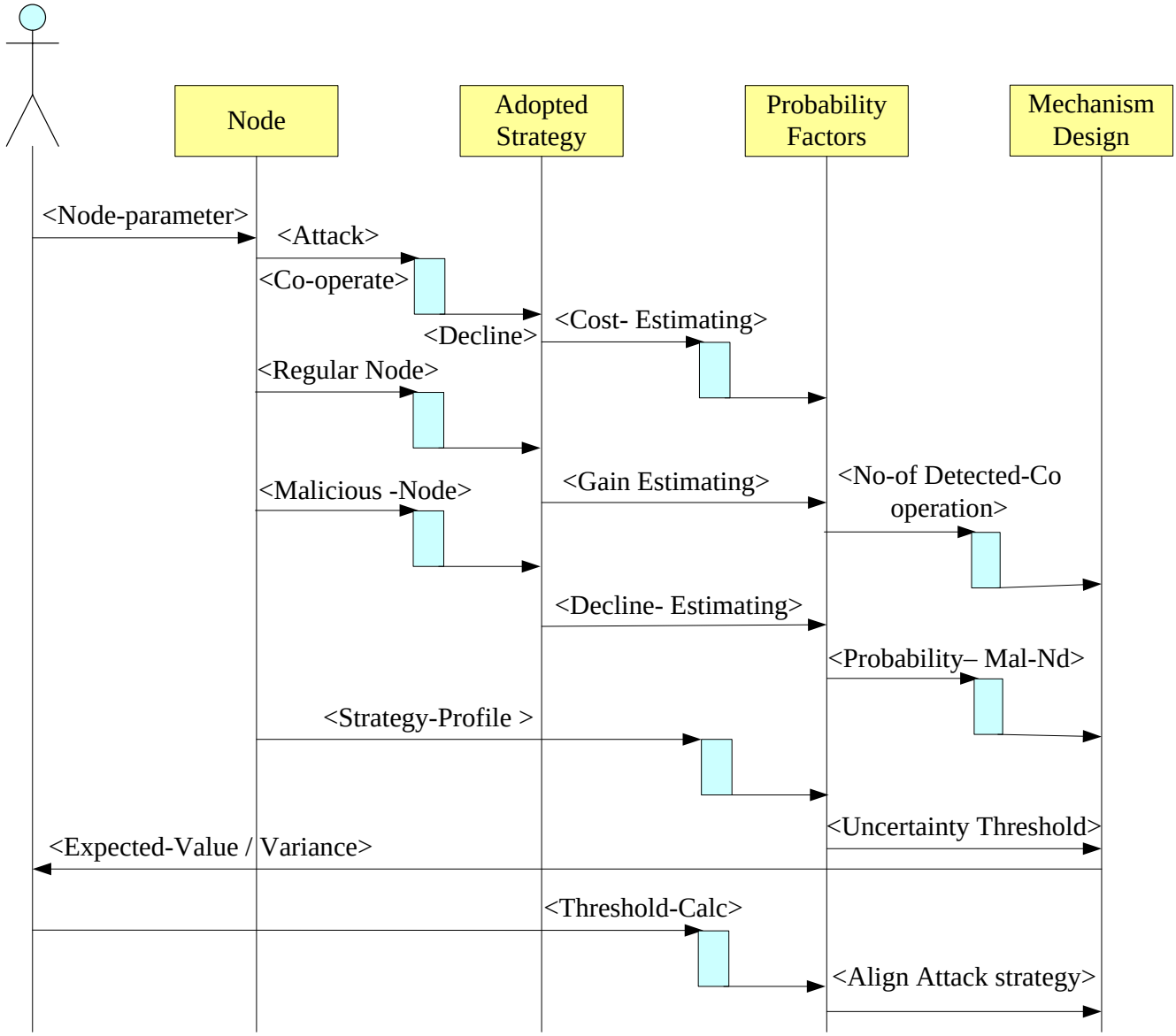

Figure 1 Strategy of the Proposed Technique

Figure 1 shows the schema of the proposed SMBP framework which is mainly categorized into two prominent design considerations, where the first category of design will stress on capturing different unpredictable malicious behaviour in MANET and the second part will stress on using programming tools to code the problems. The outcome of the study is expected to give a realistic structure of node mobility, malicious behaviour studied with respect to various clusters considered in the work. The result is also expected to achieve higher degree of potential surveillance system that could possibly track each minute communication and mobility behaviour in MANET. As the proposed SMBP framework is based on probabilistic method, the reliability of its result is also directly dependent on the design and consideration of the input and algorithm efficiency.

V. ALGORITHM AND RESULT EXPERIMENTAL RESULTS

The proposed SMBP framework is experimented on 32 bit Windows OS with 1.84 GHz (min) processor speed and programming platform is considered in Matlab. It is also known that 64-bit architectures perform 40% faster computation

than 32 bit architectures. Although the computer industry is encountering transition from 32-bit architectures to 64-bit architecture, but still majority of the users (academicians, researchers, commercial user, corporate users) still use 32-bit windows OS and therefore the proposed study is chosen to experiment over 32 bit windows OS. The proposed system has considered a packet drop attack as a mode of intrusion in dynamically generated mobile adhoc network in Matlab platform. The regular node is considered to follow its respective neighboring transmitted message by neighbor monitoring. A simulation framework of 1500×1500 m is designed with 300 mobile randomly positioned with a transmission range of 250 meters. The entire simulation area is designed with 3-9 sub-groups of communication area. A random mobility model is designed and any two nodes in the same group of communication area are considered as neighboring nodes. The objective to adopt research methodology is to generate novel insights of malicious activities. We will use the principle of constructive research which develops solutions to a problem. Here we will divide our work into two models namely theoretical model and simulation model. In the theoretical model, we will study different security issues and their solutions. In the simulation model, we will run simulation with MANET configuration and try to learn mechanisms which the help us to enforce security in Mobile Ad Hoc Networks. The figure 2 shows the implementation phase adopted.

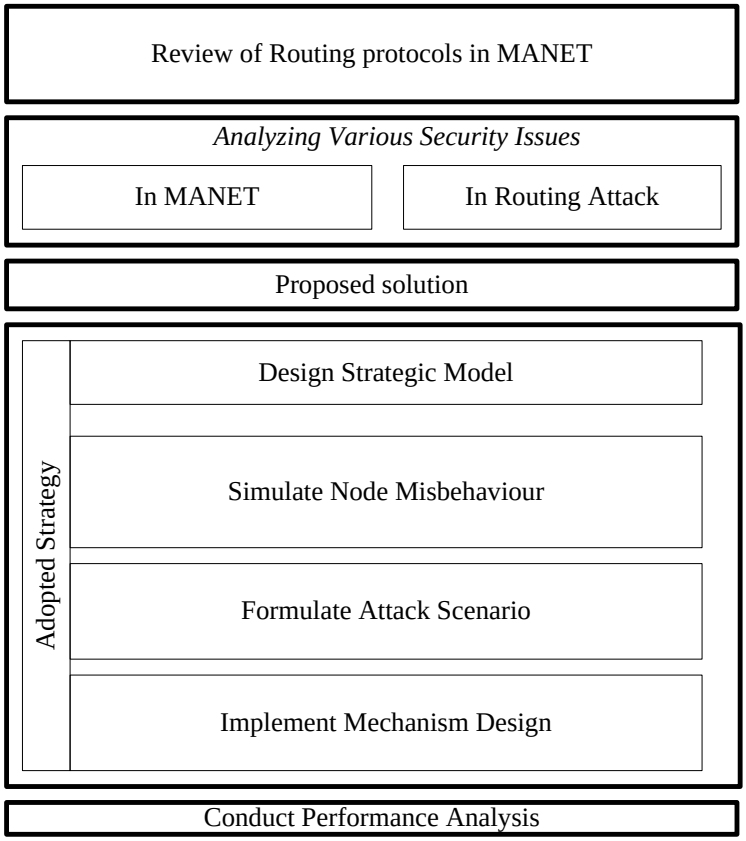

Figure 2 Proposed Plan of Implementation

The main assumptions of this study are as follows:

- The malicious nodes are totally coherent on their attack objectives.
- Probability of mistakes (false positives) in the surveillance of malicious behaviour and its observations are very low
- For the purpose of communication, the proposed SMBP framework assumes that authentication mechanism is conducted.
- In proposed SMBP framework, each mobile node is permitted to possess private data that influence the development of the routing policies. Others are assumed to have trust about the private information. Mobile nodes choose their defined actions during the routing policy according to their trust factor and private information
- Static malicious node detection routing policy is assumed to iteratively communicate at every time slot, and the SMBP framework assumes the inestimable iterative routing policies without any arrest in communication procedure.
- Time is considered to be categorized into well defined slots and each slot exhibits a stage of routing policy.
- It is assumed that node i, or the sender node, has a packet to send to node j, or the receiver node. If the sender node is regular, it only takes the action "Forward". If the sender node is malicious, it can choose to "Attack" with a risk of being identified or "Forward" to disguise

The algorithms implemented in the design of the proposed SBMP framework are as given below:

Algorithm-1: Assessing feasibility of infected mobile nodes in specified communication channel
Objective: The main objective of the algorithm-1 is to determine the feasibility of infected mobile node in the mobile adhoc network environment.

Input: *A* and *B* (*A*=Number of identified attempts of packet forwarding by normal nodes, *B*=Number of identified attempts of intrusion by malicious node)
Output: The feasibility C of infected mobile node.
Steps:
Start
Initialize identified attempt of packet forwarding by normal nodes (*A*)
Initialize identified attempt of intrusion by malicious node (*B*)
Design an operator for determining feasibility (C) of infected mobile node.
Compute feasibility (C) that the node is an infected mobile node using the equation:

$$C = B / (A + B)$$

End

Algorithm-2: Determination of Trust Factor of the system
Objective: The main objective of the algorithm-2 is to determine the trust factor by considering number of identified attempts of packet forwarding by regular nodes, attacks and unpredictability factor in the susceptible environment of MANET
Input: *A, B,* U_o
Output: Value of the trust factor of system captured during simulation study
Steps:
Start
Initialize identified attempt of forwarding packet by normal nodes (*A*)
Initialize identified attempt of intrusion by malicious node (*B*)
Initialize unpredictability factor in the opinion formulation (U_p)
Create an operator for determining the trust factor of the system
Assign ($A/(A + B)$) to D_{temp1}
Assign ($1-U_p$) to D_{temp2}
Estimate trust factor (T_F) in the opinion formulation by applying formula

$$T_F = D_{temp1} \times D_{temp2}$$

End

Algorithm-3: Determination of incredulity factor
Objective: The main objective of the algorithm-3 is to compute the incredulity of the system by considering number of detected attempts of packet forwarding by regular nodes, number of attempted attacks, and unpredictability factor in the vulnerable environment of MANET
Input: *A, B,* U_p
Output: The estimated value of the incredulity if of the system
Steps:
Start
Initialize identified attempt of forwarding packet by normal nodes (*A*)
Initialize identified attempt of intrusion by malicious node (*B*)
Initialize unpredictability factor in the opinion formulation (U_p)
Create an operator for determining the incredulity of the system
Assign ($B / (A + B)$) to D_{temp3}
Assign ($1-U_p$) to D_{temp4}
Estimate incredulity factor (I_F) in the opinion formulation by using the equation:

$$I_F = D_{temp3} \times D_{temp4}$$

End

Algorithm-4: Estimation of unpredictability factor
Objective: The main objective of the algorithm is to estimate the unpredictability factor
Input: *A, B,* U_p
Output: The algorithm gives the estimation of unpredictability factor.

Steps:
Start
Initialize identified attempt of forwarding packet by normal nodes (*A*)
Initialize identified attempt of intrusion by malicious node (*B*)
Initialize unpredictability factor in the opinion formulation (U_p)
Create an operator for determining the unpredictability of the system
Estimate unpredictability factor in the opinion (U_p) by using the equation:

$$U_p = 12 \times A \times B \ / \{(A + B)^2 \times (A+B+1)\};$$

End

The proposed algorithm is implemented in a unique coding process. Algorithm-1 is implemented when the simulation starts, i.e. node starts adopting routing policies. Algorithm-2 comes into action when there is abnormal growth of trust factor. Algorithm-3 finally confirms the value of incredulity factor of the mobile node and update the SMBP framework and thereby giving a clear picture of the node attack. Finally, the unpredictability factor in adopting an opinion for action is implemented in Algorithm-4. The simulation is performed for 200-500 mobile nodes using random distribution in the simulation area. The proposed model is evaluated for its efficiency by comparative analysis with the prior research work conducted in security of routing protocols in mobile adhoc network. For the purpose of performance comparative analysis, the proposed SMBP framework is compared with similar work done most recently by Reddy [30] and Swetha [31]. The reasons for selection of these two prior studies are as following: i) The work done by Reddy [30] has considered blackhole attacks in MANET using game theory. The results of [30] are witnessed with good packet delivery ratio, control overhead, and routing overhead, ii) the work done by Swetha [31] has considered using mechanism design for design an Intrusion Detection System in MANET, where a promising results have been accomplished.

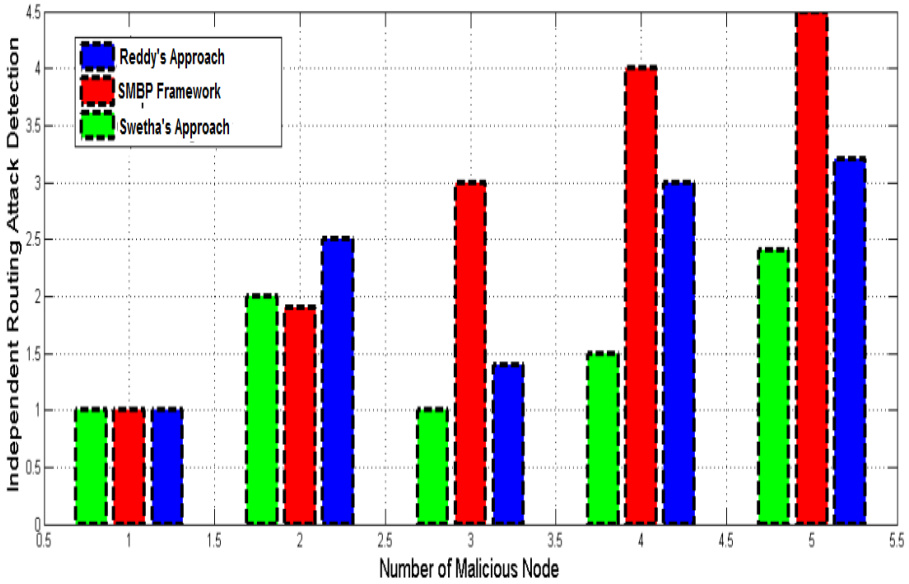

Figure3 Independent Routing Attack Detection

The Figure 3 shows the performance analysis when simulation is conducted for attack detection in independent routing. The unit of analysis has considered a scale of 100 for 1 mobile nodes in x-axis. The mobile nodes are arbitrarily attacked independently causing the aggravation of malicious nodes to initiate routing attack. However, the proposed system has higher detection rate as compared to other research work considered.

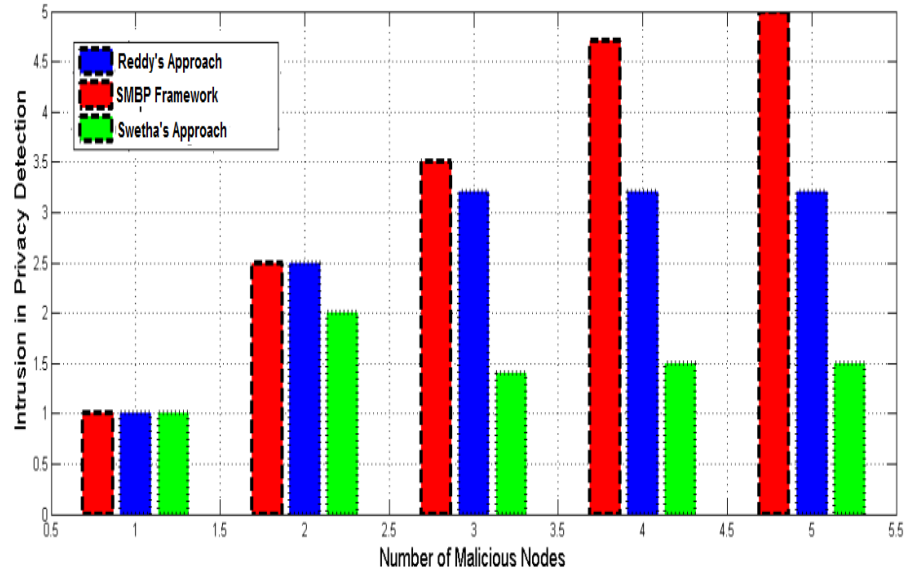

Figure 4 Intrusion in Privacy in routing attack

Figure 4 shows the performance analysis for intrusion in privacy policy maintained at each mobile node. As the routing attack has iterative and sequential propagation model, so quantity of the infected routes are maximized in terms of cost. It can also be seen that by introducing the proposed protocol, the performance of attacker for initiating routing attack is reduced by maximizing the improbability in route susceptibility.

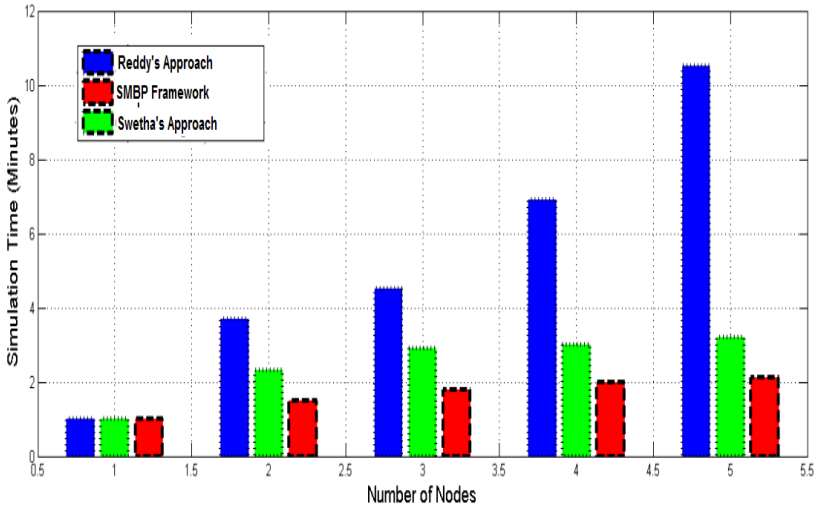

Figure 5 Simulation Speed comparisons

The efficiency of the proposed algorithm is tested by observing the simulation speed required for identifying the routing attack in mobile adhoc network along with increase of number of malicious nodes at the run time of simulation result are shown in the Figure 5. Although dynamic topology of mobile adhoc network posses issues in the design and implementation of the algorithm, but the challenge becomes more sophisticated by introducing more number of user defined multiple attack mobile nodes at the run time of the simulation. This experiment is done to check the efficiency of the proposed algorithm to identify multiple tactics adopted by intruder node. The simulation result in Figure 5 clearly shows that proposed system takes comparatively less time. The graphical analysis also shows highest peak for results in [30] obtained by neural network approach due to inclusion of learning phase of the algorithm, which consumes enough time for performing simulation. This fact should be kept in mind as propagation of the routing attack is very much faster which starts infecting even in a matter of few seconds depending upon the security loopholes factor existing in the wireless network. It can be clearly seen that the proposed algorithm yields result better contrastive results in comparison to most frequently used algorithms used in current research for analyzing the security issues in routing protocol in mobile adhoc network. The implementation of the proposed system facilitates the better visualization for route susceptibility; however, an efficient route susceptibility parameter can be designed with same alteration. The design also guarantees if any compromised route is considered for analyzing routing attack by replacing the value of cumulative routes by cost estimation in the similar route including direct route considering single hop type. The cost is defined as a constant value which basically represents the amount of energy required to move to selected destination in a cluster. The cost estimation will highlight basically the impact on mobility towards the proposed framework.

VI. CONCLUSION

In this proposed work, we have used an efficient mechanism design framework to analyze the dynamic communication between regular and malicious nodes in mobile networks. The regular node forms belief, chooses the probability to cooperate with its opponent based on its belief, and follows a rational decision rule to report. The malicious node keeps evaluating the risk of being identified and exploits its intrusion strategy to avoid any punishment. The proposed framework in these routing policies is analyzed and emphasizes the advantages that malicious nodes would gain from the intrusion strategy. A malicious node detection routing policies are formulated and also post-detection routing policies played by the regular and malicious nodes. While both routing policies are of imperfect information type, the conventional routing policies have a mixed strategy and provide solutions to achieve the equilibrium.

REFERENCES

[1] A. Shajin Nargunam, M. P. Sebastian, Dynamic Security Scheme for MANET, Managing Worldwide Operations & Communications with Information Technology, 2007

[2] Ruiliang Chen, Michael Snow, Jung-Min Park, M. Tamer Refaei, and Mohamed Eltoweissy, Defense against Routing Disruption Attacks in Mobile Ad Hoc Networks, GLOBECOM 2006

[3] Shyamala Ramachandran, 2Valli Shanmugan, Impact of Sybil and Wormhole Attacks in Location Based Geographic Multicast Routing Protocol for Wireless Sensor Networks, Journal of Computer Science 7 (7): 973-979, 2011 ISSN 1549-3636

[4] Jawandhiya, P.M., Ghonge, M.M. (2010). A Survey of Mobile Ad Hoc Network Attacks.International Journal of Engineering Science and Technology, Vol. 2(9).

[5] Garg, N., &Mahapatra, R.P. (2009). MANET Security Issues.IJCSNS International Journal of Computer Science and Network Security, Vol.9, No.8.

[6] E.B. Cohen, Issues in Informing Science & Information technology, Vol.9, 2012

[7] Kannhavong, B., Nakayama, H., Nemoto, Y., (2007). A Survey of routing attacks in mobile ad hoc networks. IEEE Wireless Communications, Page 86.

[8] Y. Hu, D. Johnson, and A. Perrig (2003). SEAD: secure efficient distance vector routing for mobile wireless ad hoc networks. Ad Hoc Networks,IEEE.

[9] Mishra, D., Jain, Y.K., Agrawal, S. (2009).Behavior Analysis of Malicious Node in the Different Routing Algorithms in Mobile Ad Hoc Network.International Conference on Advances in Computing, Control, and Telecommunication Technologies.

[10] Dasgupta, M., Choudhury, S., Chaki, N. (2010). Routing Misbehavior in Ad Hoc Network, International Journal of Computer Applications, Volume 1, No. 18

[11] Karjee, J., Banerjee, S. (2008).Tracing the Abnormal Behavior of Malicious Nodes in MANET,IEEE

[12] Crepeau, C., Davis, C.R., & Maheswaran, M.(2007).A secure MANET routing protocol with resilience against byzantine behaviours of malicious or selfish nodes.IEEE 21st International Conference on Advanced Information Networking and Applications Workshops.

[13] Wang, Li., Goa, F. (2010). A Secure Clustering Scheme Protocol for MANET, IEEE

[14] Li,W., Joshi, A., &Finin, T. (2010).Coping with Node Misbehaviors in Ad Hoc Networks: A Multi-Dimensional Trust Management Approach.IEEE Eleventh International Conference on Mobile Data Management.

[15] Gong, W., You, Z., Chen, D., (2009). Trust Based Malicious Nodes Detection in MANET, IEEE

[16] Orallo, E.H., Olmos, M.D.S., Cano, J.C., (2012). Collaborative Watchdogs: A Fast and Efficient Approach to Deal with Selfish Nodes in MANETs, IEEE.

[17] Manchikalapudi,V.,Yelisetti, S.,Surapaneni, R.K. (2012). Detecting misbehavior nodes and trust levels in MANETS, IEEE International Conference on Engineering Education.

[18] Beghriche, Y., Toubiana, V., &Labiod, H. (2008). A Bayesian filter to detect misbehaving nodes in MANETs, IEEE, New Technologies on Mobility & Security, pp.1-5

[19] Paramasivan, B., Pitchai, K.M. (2011). Comprehensive Survey on Game Theory based Intrusion Detection System for Mobile Adhoc Networks, IJCA Special Issue on Network Security and Cryptography.

[20] Sharma, K., Khandelwal, N., Prabhakar,M. (2011).An Overview Of security Problems in MANET, IJCA.

[21] F. Kargl, A. Klenk, S. Schlott, and M. Weber, Advanced Detection of Selfish or Malicious Nodes in Ad hoc Networks, 1st European Workshop on Security in Ad-Hoc and Sensor Networks (ESAS 2004)

[22] [22] A.Rajaram, S.Palaniswami, Detecting Malicious Node in MANET Using Trust Based Cross-Layer Security Protocol, (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 1 (2) , 2010, 130-137

[23] S. Marti, T.J.Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," Proc. MobiCom 2000

[24] K. Paul and D. Westhoff, "Context Aware Detection of Selfish Nodes in DSR based Ad-hoc Networks," Proc. GlobeCom 2002.

[25] K. Balakrishnan, J. Deng, and P. K. Varshney, "TWOACK: preventing selfish in mobile ad hoc networks," Proc. WCNC'05, 2005

[26] Li Zhao and José G. Delgado-Frias, MARS: Misbehavior Detection in Ad Hoc Networks, IEEE GLOBECOM 2007 proceedings.

[27] W. Lou, W. Liu, and Y. Fang, "SPREAD: enhancing data confidentiality in mobile ad hoc networks," IEEE INFOCOM 2004, pp. 2404 – 2413.

[28] K. Stewart, T. Haniotakis, and S. Tragoudas, "A security protocol for sensor networks," Proc. IEEE GlobeCom 2005

[29] http://en.wikipedia.org/wiki/Mechanism_design

[30] B. Prabhakara Reddy, M.N. Giri Prasad, Defending Blackhole Attacks In Mobile Ad Hoc Networks Using Non-Zero Game Theory, International Journal of Advances in Engineering & Technology, Vol. 6, Issue 4, pp. 1653-1663 , Sept. 2013

[31] E. Swetha, K. Sangeethasupriya, Intrusion Detection System in MANET with Secure Leader Election Model, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 7, July 2013

