Semantic Probabilistic Modelling of novel routing Protocol with Implication of Cumulative Routing Attack in Mobile adhoc network

Anil G. N.
Asst. Prof: Dept of CSE.
BMS Institute of Technology
Bangalore, India

Dr. A. Venugopal Reddy
Prof. & Principal,
University College of Engineering, Osmania University
Hyderabad, India

***Abstract*— The proposed system presents a novel approach for modelling along with mitigating various types of routing attacks in mobile adhoc network considering AODV protocol. Majority of the previous research work are either explored differently for security or routing protocols. The system identifies the susceptibility of the routing attack over the dynamic topology of mobile adhoc network where it has assumed a faster propagation of the infection towards the nodes. To make the analysis more challenging, the protocol also designs a sophisticated adversary module which is resilient against any types of preventive measure being adopted. The proposed system therefore used probabilistic approach for modelling the routing attack scenario over MANET. The uniqueness is that majority of the prior research work has focused on one type of routing attack, whereas the proposed system is experimentally evaluated for cumulative routing attack. The simulation results show highly contrastive result when compared with frequently used current algorithm for mitigating routing attacks.**

Keywords-Routing Attack, Mobile Adhoc Network, Security, AODV, Probabilistic approach

I. INTRODUCTION

Mobile Adhoc Network consists of independent wireless mobile nodes which group together to form a momentary wireless network without any assistance of any centralized management or fixed infrastructure. Internet Engineering Task Force (IETF) has MANET working group (WG) that is devoted for developing IP routing protocols [1]. One of the huge concerns in mobile adhoc network is the maintaining efficient, robust, and secure routing protocols, which has attracted many researchers. Routing protocols are normally required for maintaining efficient transmission among the mobile nodes by exploring the network topology, which in this case is always dynamic. It also designs a route for pushing the data packets and also manages the routes among the pair of mobile nodes. One of the fundamental problem with majority of the routing protocol is that the routing protocol relies on all the mobile nodes present in the network and depending on the situation that these mobile nodes will perform or collaborate appropriately; but there is a higher feasibility of circumstances where certain specific set of nodes may not behave appropriately giving rise to suspicious factor. Unfortunately, majority of the routing protocols in mobile adhoc network is witnessed for declined performance at the time of communicating with large scale of misbehaving nodes, which definitely sustains the course of route exploration but also disrupt the course of data rendering the routing protocol to resume again the route exploration procedure or to chose an unconventional route in case it is available. Moreover the newly opted route has the feasibility of possessing a few malicious nodes, resulting in failure of new route too. Such methodology iterates till the sender node confirms that the data will not be able to transmit ahead. The fundamental issue with frequently used routing protocols is that they rely all mobile nodes of network and based on the assumption that nodes will behave or cooperate properly but there might be a condition where some nodes are not behaving properly. Majority of the adhoc network routing protocols becomes inefficient and shows reduced performance while mitigating with big number of misbehaving nodes. Such set of misbehaving nodes support the flow of route discovery traffic but interrupt the data flow, causing the routing protocol to restart the route-discovery process or to select an alternative route if one is available.

Mobile adhoc network should posses a better and effective security as various upcoming application based on MANET are on its way in future. Mitigating the routing issues will create a better, efficient, and secure application in mobile adhoc network. Various types of attacks in mobile adhoc network like Wormhole attack, Black hole attack, Sybil attack, flooding attack, routing table overflow attack, Denial of Service (DoS), selfish node misbehaving, impersonation attack etc. has to be researched on more for better result. The proposed paper will present a framework for mitigating majority of the types of routing attack using probabilistic approach. The proposed system has large dimension of testing conducted to check the efficiency of routing protocol using AODV on majority of routing attack in mobile adhoc network.

In Section II, we will discuss about the previous research work in this area followed by Section III about various categories of routing attack. Section IV highlights proposed system followed by implementation in section V. In depth discussion of research performance analysis is done in section-VI followed by conclusion in section-VII.

II. RELATED WORK

Recently, numerous approaches have been proposed to deal with the node non-cooperation problem in wireless networks. They generally can be classified into two main categories: reputation systems and price-based systems. We use a monitoring and reputation system [2] as the basic setting for regular nodes. Many related works also use reputation systems [3]–[5] and a game theory model [6] to analyze the problem. Some recent works have studied the incentives for malicious nodes and modeled their behavior more rationally. In [7], Liu et al. present a general incentive-based method to model the attackers' intents, objectives, and strategies. In [8], Theodorakopoulos and Baras further study the payoff of the malicious nodes and identify the influence of the network topology. However, the good nodes' behavior in [9] is simple, and it fails to consider the possibility that an attacker might choose different attack frequencies toward different opponents.

The security problem and the misbehaviour problem of wireless networks including MANETs have been studied by many researchers e.g. [9], [10], [11], [12].Various techniques have been proposed to prevent selfishness in MANETs. These schemes can be broadly classified into two categories: credit-based schemes and reputation based schemes. The basic idea of credit-based schemes is to provide incentives for nodes to faithfully perform networking functions. Nodes get paid for providing services to other nodes. When they request other nodes to help them for packet forwarding, they use the same payment system to pay for such services.

Sanjeev Rana [13] has created a mechanism with the help of which it prevents various replay attacks and also activate the neighboring nodes to control the behavior of its neighbors to thwart active attacks. Rakesh Kumar e.t. al [14] has implemented a prototype of key management service by using genetic algorithm. Rajib Das e.t. al [15] has proposed a solution against black hole attack and has illustrated the effect of black hole attack on network performance. However, the results cannot be considered as optimal. Kannan e.t. al [16] has published an extensive survey on various attacks, and their respective countermeasures with respect to vulnerability in routing protocols. Aishwarya Sagar [17] has proposed an approach based on reputation system that deals with routing misbehaviour and consists of identification and separation of misbehaving nodes. Hariharan e.t. al [18] has proposed a new technique termed as recommendation based on identification of routes with misbehaved nodes. Usman e.t. al [19] have analyzed the effects of different types of jammers using Conservation of Flow (CoF), which has been useful for detecting other attacks, in the wired networks. Abbas [20] have categorized reputation based schemes based on monitoring approaches: active and passive based acknowledgments. Finally, the authors have discussed their pros and cons as well as some other important identity related issues.

Depending of the patterns of the intrusion, attacks towards mobile adhoc network can be categorized into active or passive attack. Not only this, the attacks can be also further classified into internal or external attack. In association with the victim node, the attack can be again classified into routing packet or data packet attacks. In case of routing packet attack, the malicious node resist existing routes from being utilized and also it spoofs other non-existing routes for alluring data packets to be forwarded to them.

Although there are number of research conducted in past [21],[22],[23], [24], [25] for analyzing routing attacks on mobile adhoc network. Important routing attacks are fabrication, blackhole, and alteration of various fields in routing packets e.g. RREQ, RREP, RERR message, etc. Research work conducted in [26], [27], [28] discusses about some mitigating techniques for safeguarding the routing protocols in mobile adhoc network. Although these set of research work can successfully resist illegitimate nodes from participating the network, but unfortunately, it was found to increase the significant network overhead with respect to key exchange as well as authentication with restricted intrusion eradication.

The resistance based approach are also found less efficient for mitigation from malicious intruders who already have the confidential information for rendering communication by themselves in the mobile adhoc network. The prior research work has also seen the introduction of Intrusion Detection System for mobile adhoc network. Unfortunately, due to the dynamic topology of mobile adhoc network, majority of such research work are modeled to be scattered and possesses cooperative data-structure.

Specification-based approaches, for example DEMEM [29], C. Tseng et al. [30] and M. Wang et al. [31], monitor network activities and compare them with known attack features, which are impractical to cope with new attacks. A completely new work done in same field called as Intrusion Response System in mobile adhoc network has being discussed in [32] which detaches the malicious node, once identified, depending on their reputation system. Unfortunately, the work fails to be at par with efficient IDS system. The Table.1.will highlight specifically all the prominent research work being done towards securing routing protocol in mobile adhoc network.

Table.1. Prior research work

Year	Authors	Problem Focused	Approaches used	Results Obtained
2009 [33]	M.K. Jeya Kumar R.S. Rajesh	Cumulative routing Issues	Designed a mobility model using Random waypoint	AODV performs better than other routing protocols.
2009 [34]	Abdul Rahman Zuriati Zukarnain	Link breakage	Designed a mobility model using Random waypoint	AODV performs better than other routing protocols.
2009 [22]	Nishu Garg R.P.Mahapatra	Performance degradation due to routing issues	Just discussed about security consideration for effective routing	Not optimized result
2009 [35]	Dipankar Deb Srijita Barman Roy Nabendu Chaki	GPS-free positioning systems	Designed Location Aided Cluster Based Energy-efficient Routing	Lowering mean hop and hence in utilizing the limited energy of mobile nodes.
2009 [36]	E.A.Mary Anita V.Vasudevan	Black hole attack	Designed Security in Multicast Ad-hoc On Demand Distance Vector	Better result for Black Hole attack only
2009 [37]	Ashwani Kush P. Gupta C.Jinshong. Hwang	Security in Routing protocol	Designed a Power Aware Virtual Node Routing Protocol	Not optimized result Increases Network Overhead
2009 [38]	Sheenu Sharma Roopam Gupta	Black hole attack	measuring the packet loss in the network with and without a blackhole	Only 26% reduction in network performance in presence of Blackhole attack
2009 [39]	Cong Hoan Vu, Adeyinka Soneye	Collaborative Black hole Attacks	Designed a simulation to check the performance	Only resistive against Blackhole attack.
2010 [40]	Irshad Ullah Shoaib ur rehman	Black hole attack	Studying Blackhole attack on OLSR and AODV	Is not effective on DSR, TORA, GRP etc.
2010 [41]	Shishir K. Shandilya Sunita Sahu	RREQ Flooding Attack	Designed a distributed cooperative model in which all the node locally run the intrusion detection code and cooperate with each other to detect and prevent flooding attack in the network.	Results completely dependent on threshold value. The proposed result delays the detection of misbehaving node
2010 [42]	Akanksha Saini Harish Kumar	Effect Of Black Hole Attack On AODV	Designed a simulation to check the performance	The experiment didn't reached the better results for ensuring protection from blackhole attack on AODV routing protocol
2010 [43]	Aishwarya Sagar Anand Ukey Meenu Chawla	Packet Dropping Attack Routing Misbehavior	Designed a simulation to check the performance	Results doesn't guarantee that ACK packets are genuine and no work done in punishing misbehaving nodes.
2010 [44]	Moitreyee Dasgupta Choudhury Chaki	Routing Misbehavior Impact of rushing attack implemented by malicious nodes (MNs) on AODV routing protocol	Designed RREQ forwarding mechanism	Better result for Rushing attack only however.
2011 [45]	Kannan Maragatham	Study of various attack	Just a theoretical Paper	-N/A
2011 [46]	Amrit Suman	Work hole attack	analyze three ad-hoc routing protocols AODV, DYMO, FISHEYE against wormhole attack in wireless network.	Better result for worm hole attack

III. ROUTING ATTACKS

The prominent job of the routing protocol is to explore the topology in order to ensure that every node can get the access on current map of the network for designing routes in its destination. The routing attack can be represented as shown in Fig.1. where a malicious node (MN) can completely absorb the network traffic by introducing themselves within the network link of sender node to recipient node along with intermediate nodes (IN-1, IN-2) and thereby possessing the unauthorized control over the mobile adhoc network.

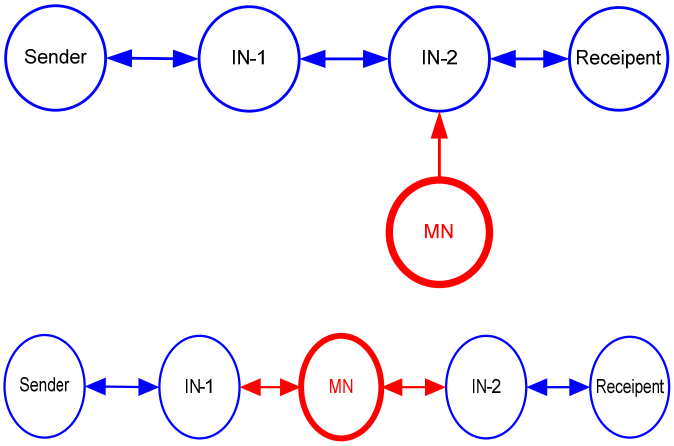

Fig.1. Representation of Routing Attack

The theoretical understanding of the attacks in network layer can be classified as routing attack and packet forwarding attack [47]. The concept of routing attack will be related to performing any activity for broadcasting updates on routing which do not trail the configuration of the specified routing protocols where the particular attack pattern is associated to the routing algorithm deployed by mobile adhoc network. The infected or malicious routing nodes can initiate an attack in mobile adhoc network by deploying different ways. Some of the major type of the routing attack as follows:

1. *Routing Table Overflow Attack*: It normally takes place in proactive routing algorithm. The main purpose of this type of attack is to create big set of routes so that designing of new routes can be resisted.

2. *Routing Table Poisoning*: in this type of attack, the malicious node forwards fake routing updates resulting in routing table poisoning.

3. *Packet Replication*: Here the malicious node duplicates the out of date packets for consuming bandwidth and unwanted resource consumption.

4. *Rushing Attack*: Such attack is highly targeted on on-demand routing protocol.

5. *Route Cache Poisoning Attack*: It uses the benefit of promiscuous mode of updating routing table, which normally occurs when confidential information within the routing table is either modified, erased, or maliciously written with fake information.

Attacks on Particular Routing Protocol

Various attack has been reported in the prior research work which is very much specific to the commonly used routing protocol in mobile adhoc network which only surfaces due to designing services of routing without assuming prime issues in security. The routing protocols specific to the attack are as follows:

1. *AODV*: The adhoc on-demand distance vector is reactive routing algorithm, where the attacker [22] all attempt to broadcast a route with less distance parameter than original or broadcast a fake routing information to disrupt the routing.

2. *DSR*: Dynamic Source Routing which is almost similar to AODV, where it is highly feasible to alter the source route listed in the control message (RREQ, RREP) by the attacker.

3. *ARAN*: Authenticated Routing for Adhoc Network is also a type of on-demand routing protocol. Although, ARAN has some best features for security in adhoc network, but still it cannot stand for rushing attack.

4. *ARIADNE*: It is also an on-demand secure routing protocol which is based on dynamic source routing. Although ARIADNE is robust for denial of service attack, but still it cannot mitigate wormhole and rushing attack [48].

5. *SEAD*: It is designed on Destination Sequence Distance vector. It can encounter against replay attack using cost effective cryptographic algorithm, but it cannot stand against wormhole attack [48].

Other types of attacks commonly found in literature are Wormhole Attack, Blackhole Attack, Byzantine Attack, Rushing Attack, Resource Consumption Attack, and Location Disclosure Attack

Countermeasures for Routing Attacks

The vulnerability of the network layer is very highly prone for routing attack in comparison to other layers in mobile adhoc network, which induces a diversified threats in security. Deploying algorithms in security considering routing protocols will only facilitate the countermeasures against such lethal attack which is very difficult to identify. Source authentication as well as message integrity technique can be

used for non-passive attack e.g. modification of routing information content. Use of message authentication code, digital signature, hashed MAC as well as one-way hash MAC key chain can be deployed for such mitigation technique. While wormhole attack can be mitigated by using unchangeable and self-sufficient physical parameter e.g. delay in time and geographical position. The work done in [49] already proved adoption of packet leashes for mitigating such issues. Another most frequently used technique is IPSec on network layer in world wide web to facilitate definite layer of privacy and security. ARAN is another efficient routing protocol which provides protection from various types of attacks e.g. corruption of hop counts, altering of sequence number, IP spoofing, DDoS, fabrication of source route [50]. Finally, work done in [51] also highlights use of security technique to mitigate blackhole attack by paralyzing the ability of reply of an intermediate mobile node, so that destination node never receives the reply message.

IV. PROPOSED SYSTEM

The proposed system presents a framework for contrastive analyzation of routing protocols where the routing attacks can be determined. Majority of the prior research work has focused on building either a mathematical model or any analytical model considering one of the type of routing attack in mobile adhoc network. The problem with such approach is that it can better thwart for one of the routing attack while become inefficient for other types of routing attack. So, due to this research gap, the proposed system has focused on designing a hybrid framework which can model almost all types of routing attack in mobile adhoc network thereby acting as an effective solution for identifying the sectors of routes which are compromised or about to be compromised.

The proposed system can be classified into following modules e.g. network model, cryptographic model, attacker model.

A. *Network Model*:

The current work of mechanizing the security in routing protocol is designed considering group of nodes N and routes R, which can be represented mathematically as G={N, R}as directed graph. The route R is completely dependent on factors like current position of node, relationship, and charecteristics of the mobile nodes, medium of communication, and MAC layer. The dispatcher and destined nodes can be depicted as D and d, which is constructed depending on decision taken by routing protocol. One or multiple routes will be designed considering set of sequential R for a given set of dispatcher node D and destined node d. Cumulative route $CR_{D,d}$ is designed for all the links considered from D to d. Let F_t signifies the part of the travel from D to d such that it travels the path $t \in CR_{Dd}$. The cumulative route CR_{Dd} can be depicted as route sub-graph G_{Dd} of G possessing mobile nodes and directed graph travelled by atleast one of the routes $t \in CR_{Dd}$. The routing protocol using AODV is designed based on segregating the spatial factors depending on packets forwarded along the diversified routes. The consideration is made for both single and multi-paths.

B. *Cryptographic Model*:

The module will be responsible for maintaining security of the packets by assigning cryptographic keys. The model considers S_{key} as group of symmetric security keys and P_{key} be equivalent group of public keys. If i be node number considered than $i \in N$, which is allocated with S'_{key} such that $S'_{key} \subseteq S_{key}$ and also public tag substitution key $P'_{key} \subseteq P_{key.}$ The common set of the keys shared among i and j as $S_{key(i,j)} = S_{key(i)} \cap S_{key(j)}$, which is the criteria for permitting transmission of packets between i and j when $S_{key(i,j)} \neq 0$. The representation is as shown in Fig.2. It is also considered that the model will use $S_{key(i,j)}$ shared keys completely in order to protect the specified route (i, j). Therefore, the proposed model should have some common keys in $S_{key(i,j)}$ for secure communication in specified route. Not only this, the model will also consider the computation of $P_{key(i,j)}$ as $P_{key}(i) \cap P_{key(j)}$ for the purpose of estimating the group of shared key $S_{key(i,j)}$.

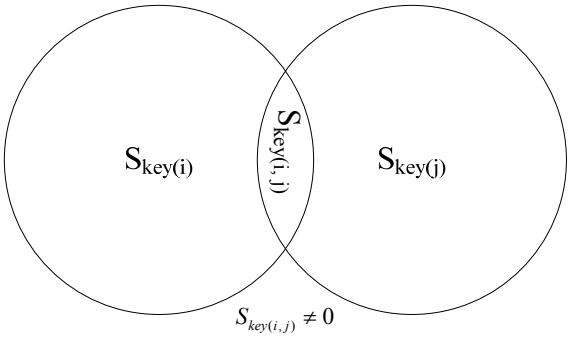

Fig.2. Set Representation of Cryptographic assumption

The category of public tag substitution design will posses any rule which facilitates required data from any other mobile nodes $j \in N$ in order to evaluate group of $P_{key.}$ as public broadcast mechanism. The security of the design of the routing protocol starts from this phase a rule is designed to provide dual layer of security for any message being communicated. This module is created to show that our attacker module is a stronger module to decrypt even this security layer, thereby assist the framework to catch hold of the attacker by determining the infected routes till that instant. This dual layer of security will facilitate data for node j for only estimating $P_{key(i,j)}$ with respect to node i without furnishing any information to other node j.

C. *Attacker Model*:

Our previous work has already focused on the modelling the behaviour of the attacker node for preventing the decamping mechanism. The uniqueness part of the proposed system is the design of this attacker module where we are considering that

this module is extremely strong enough to decrypt any of the information transacted between any authorized mobile nodes by invoking any types of routing attack. The main intention of this module is to intrude or initiate any of the routing attack along with infection spread from dispatcher node D to destined node d with minimum cost of attack. But this time the attacked module is enhance with additional capability by which they can attach an unit cost in resource expenditure needed to initiate an attack. As in mobile adhoc network, there is no digital certificate authentication among the nodes so, we also consider that this module will attempt to give rise to all issues like route disruption, node isolation, and resource consumption in the defined scenario of the mobile adhoc network and they perform all this by extracting the secure keys from the authorized nodes. The model also assumed to posses all the route information G_{Dd} using our previous model.

V. IMPLEMENTATION

The proposed system is implemented on 32-bit windows OS with 1.84 GHz dual core processor using Java Platform. The framework of the project work is has basically two stages of operation for the users. The first stage enables the user to select and configure their network choosing from key analysis, link analysis, as well as route analysis. The key analysis section is further classified into 5 different types: basic, polynomial, hybrid, broadcast, and public type. Once after proper selection of the key analysis mode, the key development mode gets surfaces in the framework, which is further divided into random (or binomial) and pulse type. Link Analysis mode operates in the same way. Route Analysis is activated along with the options of Traffic type, flow deployment, and routing type. The user can select the traffic type with an option of data collection, data distribution, and peer activity. The next option of flow deployment is provided with route to closest sink and route to random target. The last option of routing type is classified for the user into three types e.g. multipath, dependent, and end-to-end type. Once the selections is set, the action mode is activated to display the network in the simulation mode. To construct the proper network, the user has to feed the proper parameters related to the node information, which includes number of nodes, its respective deployment area, radio range, connectivity, key ring size, maximum hop cost and distance, and multipath spread per hops. Insertion of the proper parameters will check for neighborhood size, maximum connectivity, and key pool, based on which the network will be constructed. The simulated network will show the traffic, link, potential routes, key information, initiate attacks. Finally, the user can visualize the compromised values related to key, nodes, links, traffic, and route.

The proposed model also designs a route sensitivity parameter (RSP) in order to compute optimal security standard for the transmission being active on specified route CR_{Dd}. Majority of the prior research work towards security of routing in mobile adhoc network is more focused on identification of the attack only after the event of attack has already being bypassed. Such approaches are beneficial for only understanding the flaws in design of routing protocol. Unfortunately, the routing attacks on dynamic MANET scenario are very much latent within the wireless adhoc network and their propagation model is almost impossible to predict. Therefore the proposed model will use probabilistic approach for generating a various diversified routes for any given application of mobile adhoc network and visualize the effectiveness of routes by invoking attack in the routes to estimate the safe routes and unsafe routes. For the effectiveness of the result, the model will implement Greedy Heuristic Algorithm.

Algorithm: Probabilistic Model of identifying routing attack in given MANET scenario

Input: Node parameters

Output: Identification of infected routes

Steps:

1 ***Initialize*** *mobile node parameters*
2 *Define key types*
3 *{public, broadcast, polynomial, hybrid}*
4 *Define route types*
5 *{multipath, end-to-end}*
6 ***Initialize*** *maximum hop distance*
7 *Estimate neighborhood size*
8. $Size_{(neigh)} = \{(No.\ of\ Nodes)\ .(\pi).(Radio\ Range)^2\}/\ Deployment\text{-}Area$
9 *Design network module*
10 *Design Cryptographic module*
11 *Design attacker module*
12 ***Switch*** *Case (Route Susceptibility):*
13 $S_{key(i,j)} \neq 0$
14 $S_{Dd}(\phi) = 0$
15 $S_{Dd}(A_{nodes}) = 1$
16 $0 < S_{Dd}(A_{nodes}) < 1$
17 *Estimate current values of all parameters*
18 ***If*** *Cost in reduced and* $S_{Dd}(A_{nodes}) = 1$
19 *Estimate Anodes and* CR_{Dd}.
20 *Estimate Cost*

$$\sum_{i \in A_{nodes}} Cost_i$$

21 ***Else***
22 ***Go*** *to Step (18)*
23 *Estimate probabilistic infected routes*

$$\sum_{i \in N} \frac{S_i(A_{nodes})}{Cost_i}$$

24 ***End***

The proposed model will estimate the impact of routing attack on the designed security routing protocol considering specified cumulative route CR_{Dd} with the initiation of attack on group of nodes $A_{nodes} \subseteq N$. Let us consider $S_{key(comp)}$ as group of keys being corrupted by the attacker module, which will mean that any packets transmitted through CR_{Dd} which was already encrypted with $S_{key(i)}$ or $S_{key(j)}$ will definitely get compromised by the malicious nodes present within that route. The considered route (i, j) or (D, d) ϵ P_{key} is attacked if and only if

$S_{key(i,\ j)} \subseteq S_{key(comp)}$ and let $P_{key(comp)}$ represents all the attacked routes. Therefore the design of attack on complete route from dispatcher node D to destined node d will represent that any message being communicated using the specified route will definitely get corrupted by the A_{node}. Not only this, the design of the proposed routing protocol also considers the route susceptibility for routing attack when it comes under any of the following criteria:

- $S_{Dd}(\phi) = 0$, which means there is no attack if there is no routes from Dispatcher node D to destined node d.
- $S_{Dd}(A_{nodes}) = 1$, which means that CR_{Dd} is only attacked when there is presence of atleast 1 A_{nodes}.
- $0 < S_{Dd}(A_{nodes}) < 1$, which means the maximum and minimum intensity of attack considering complete route is not attacked but only a portion of it is infected due to routing attack.

VI. Performance Analysis

The simulation is performed for 200 mobile nodes using random distribution in the simulation area. The model is designed considering the arbitrary allocation of 45 keys. The proposed model is evaluated for its efficiency considering comparative analysis with the prior research work conducted in security of routing protocols in mobile adhoc network. The frequently used approaches are Genetic Algorithm [52], Neural Network [53][54], Artificial Immune System [55][56], and Classification Algorithm [57] using Support Vector Machine (SVM).

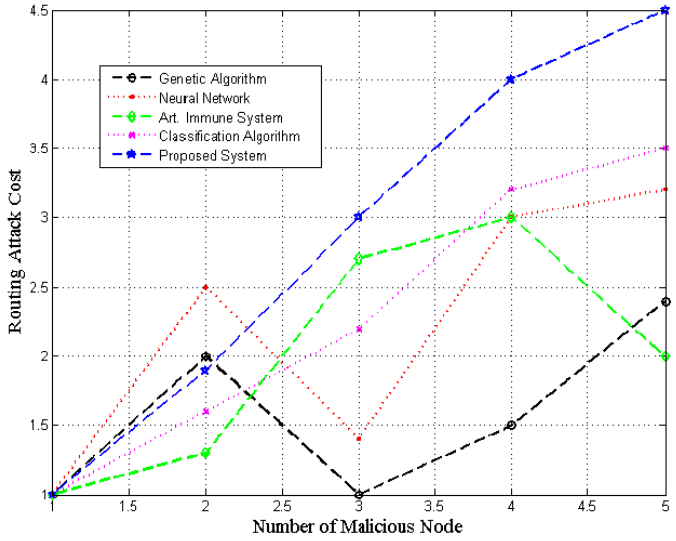

Fig.3. Independent Routing Attack

The Fig.3. shows the performance analysis when conducted for independent route. The bottom line is 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 prior research work shown.

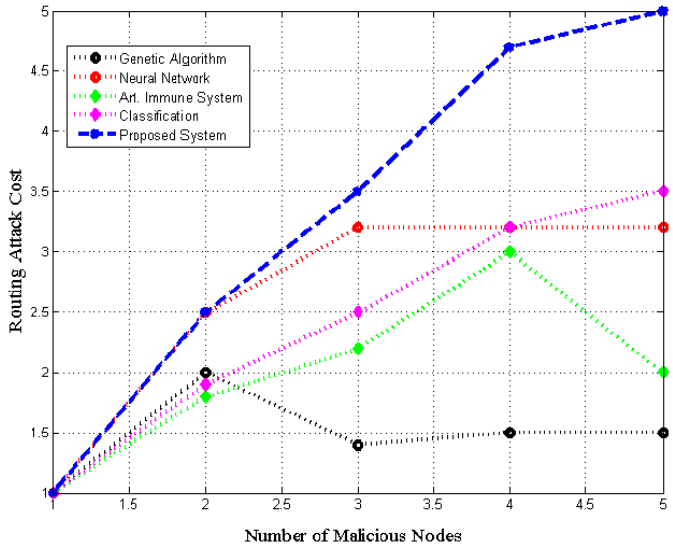

Fig.4.Intrusion in Privacy in routing attack

Fig.4. shows the performance analysis for intrusion in privacy policy maintained at each nodes. 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.

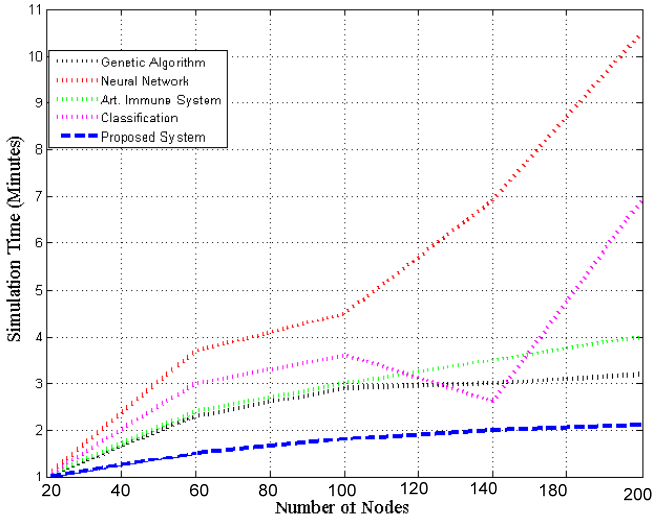

Fig.5. Simulation Speed comparison

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 as shown in Fig.5. Already consideration of dynamic topology of mobile adhoc network posses issues in the design and implementation of the algorithm, but the challenge portion of the performance analysis is made more sophisticated by

introducing more number of user defined multiple attack mobile nodes (A_{nodes}) at the run time of the simulation. This experiment is done to check the efficiency of the proposed algorithm to identify many attack variables which is not even programmed. The simulation result in Fig.5. clearly shows that proposed system takes comparatively less time. The graphical analysis also shows highest peak for 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 faster which starts infecting even in a matter of seconds depending upon the existing security loophole factor existing in the wireless network. It can be clearly seen that the proposed algorithm has better contrastive result 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 slight alteration. The design also guarantees if any compromised route is considered for analyzing routing attack by replacing CR_{Dd} by cost estimation in the similar route including direct route considering single hop type (D, d). The routing attack on unit route vector $t \in CR_{Dd}$ is more than enough for permitting the attacker to recuperate a portion F_t of the route from D to d.

VII. CONCLUSION

The proposed paper has examined the issues in designing new efficient and secure routing protocol considering all the routing attack susceptibility parameter in order to enhance the efficiency of the proposed protocol using AODV. A mathematical model is design with algorithm for estimating the impact of majority of the routing attack on mobile adhoc network using probabilistic approach using greedy heuristic algorithm. A sophisticated attacker module is design which can initiate a routing attack in our case in order to understand whether the proposed algorithm can efficiently trace the infected routes. Majority of the implementation done by enhancing cryptographic approach is considered to increase the network overhead which results in poor performance in the network. But our algorithm executes in less than 2 minutes to simulate a large scale scenario of routing attack in user-defined consideration of mobile adhoc network. Therefore, we have evaluated the simulation speed of the proposed design by adding up multiple malicious nodes at the runtime of the simulation. A comparative analysis is performed with proposed system against most frequently used algorithm like Genetic Algorithm, Neural Network, Artificial Immune System, Classification Algorithm using SVM to see that our system has contrastive result in comparison.

.

REFERENCE

[1] http://www.ietf.org/dyn/wg/charter/manet-charter. Accessed on 6th Dec, 2011
[2] S. Buchegger and J. Boudec, “A robust reputation system for P2P and mobile ad-hoc networks,” in Proc. 2nd Workshop Econ. Peer-to-Peer Syst., 2004, pp. 403–410.
[3] F. Li and J. Wu, “Mobility reduces uncertainty in MANETs,” in Proc. IEEE INFOCOM, 2007, pp. 1946–1954.
[4] A. Josang, R. Ismail, and C. Boyd, “A survey of trust and reputation systems for online service provision,” Decis. Support Syst., vol. 43, no. 2, pp. 618–644, Mar. 2007.
[5] F. Li, A. Srinivasan, M. Lu, and J. Wu, “Uncertainty mitigation for utility-oriented routing in MANETs,” in Proc. IEEE GLOBECOM, 2007, pp. 427–431.
[6] F. Li and J. Wu, “Hit and run: A Bayesian game between malicious and regular nodes in mobile networks,” in Proc. IEEE SECON, 2008, pp. 432–440.
[7] P. Liu, W. Zang, and M. Yu, “Incentive-based modeling and inference of attacker intent, objectives and strategies,” ACM Trans. Inf. Syst. Secur., vol. 8, no. 1, pp. 78–118, Feb. 2005.
[8] G. Theodorakopoulos and J. Baras, “Malicious users in unstructured networks,” in Proc. IEEE INFOCOM, 2007, pp. 884–891.
[9] Kejun Liu, Jing Deng, Pramod K. Varshney, and Kashyap Balakrishnan, “An Acknowledgment-Based Approach for the Detection of Routing Misbehaviour in MANETs”, IEEE Transactions on mobile computing, Vol. 6, NO. 5, May 2007.
[10] Dhanalakshmi, Dr.M.Rajaram ,” A Reliable and Secure Framework for Detection and Isolation of Malicious Nodes in MANET”, IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.10, Oct2008
[11] Zan Kai Chong, Moh Lim Sim, Hong Tat Ewe, and Su Wei Tan ,” Separation of Detection Authorities (SDA) Approach for Misbehavior Detection in Wireless Ad Hoc Network”,PIERS Online, VOL. 4, NO. 8, 2008.
[12] S. Buchegger and J.-Y. Le Boudec, “Performance Analysis of the CONFIDANT Protocol: Cooperation of Nodes, Fairness in Dynamic Ad-Hoc Networks,” Proc. MobiHoc, June 2002.
[13] Sanjeev Rana, Manpreet Singh, “Performance Analysis of Malicious Node Aware Routing for MANET using Two-Hop Authentication”, International Journal of Computer Applications (0975 – 8887), Volume 25– No.3, July 2011
[14] Rakesh Kumar, Piush Verma, Yaduvir Singh, “Design and Development of a Secured Routing Scheme for Mobile Adhoc Network”, International Journal of Computer Applications (0975 – 8887) Volume 13– No.2, January 2011
[15] Rajib Das, Bipul Syam Purkayastha, Prodipto Das, “Security Measures for Black Hole Attack in MANET: An Approach”, International Journal of Engineering Science and Technology (IJEST), 2011

[16] S. Kannan, T. Maragatham, S.Karthik, V.P. Arunachalam, "A study of Attacks, Attack Detection, and Prevention Methods in Proactive and Reactive Routing Protocols", International Business Management, 2011
[17] Aishwarya Sagar, Anand Ukey, Meenu Chawla, "Detection of Packet Dropping Attack Using Improved Acknowledgement Based Scheme in MANET", IJCSI International Journal of Computer Science Issues, Vol. 7, Issue 4, No 1, July 2010
[18] Sowmiya Hariharan, Jothi Precia, Suriyakala.C.D, Prayla Shyry, "A Novel Approach for Detection of Routes with Misbehaving Nodes in Manets", International J. of Recent Trends in Engineering and Technology, Vol. 3, No. 2, May 2010
[19] Usman Yaseen, Ali Zahir, Faraz Ahsan, and Sajjad Mohsin, "Estimating the Effects of Jammers via Conservation of Flow in Wireless AdHoc Networks", International Journal for Advances in Computer Science, Volume 1, Issue 1, 2010
[20] Sohail Abbas, Madjid Merabti, and David Llewellyn-Jones, "A Survey of Reputation Based Schemes for MANET", The 11th Annual Conference on The Convergence of Telecommunications, Networking & Broadcasting (PGNet 2010), Liverpool, UK, 21-22 June 2010
[21] Pradip M. Jawandhiya et. al. / International Journal of Engineering Science and Technology Vol. 2(9), 2010, 4063-4071.
[22] Nishu Garg and R.P.Mahapatra, "MANET Security Issues ," IJCSNS International Journal of Computer Science and Network Security, VOL.9 No.8, August 2009.
[23] B. Kannhavong, H. Nakayama, N. Kato, A. Jamalipour, and Y. Nemoto. A study of a routing attack in OLSR-based mobile ad hoc networks. International Journal of Communication Systems, 20(11):1245–1261, 2007.
[24] B. Kannhavong, H. Nakayama, N. Kato, Y. Nemoto, and A. Jamalipour. A collusion attack against olsr-based mobile ad hoc networks. In GLOBECOM, 2006.
[25] B. Kannhavong, H. Nakayama, Y. Nemoto, N. Kato, and A. Jamalipour. A Survey of routing attacks in mobile ad hoc networks. IEEE Wireless Communications, page 86, 2007.
[26] Y. Hu, A. Perrig, and D. Johnson, "Ariadne: A Secure On-Demand Routing for Ad Hoc Networks," Proc. of MobiCom 2002, Atlanta, 2002.
[27] Y. Hu, D. Johnson, and A. Perrig. SEAD: secure efficient distance vector routing for mobile wireless ad hoc networks. Ad Hoc Networks, 1(1):175–192, 2003.
[28] Y. Hu, A. Perrig, and D. Johnson. Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks. Wireless Networks, 11(1):21–38, 2005.
[29] C. Tseng, S. Wang, C. Ko, and K. Levitt. Demem: Distributed evidence driven message exchange intrusion detection model for manet. In Recent Advances in Intrusion Detection, pages 249–271. Springer, 2006.
[30] C. Tseng, T. Song, P. Balasubramanyam, C. Ko, and K. Levitt. A Specification-Based Intrusion Detection Model for OLSR. LECTURE NOTES IN COMPUTER SCIENCE, 3858:330, 2006.
[31] M.Wang, L. Lamont, P. Mason, and M. Gorlatova. An effective intrusion detection approach for OLSR MANET protocol. In Secure Network Protocols, 2005.(NPSec). 1st IEEE ICNP Workshop on, pages 55–60, 2005.
[32] T. View. Information theoretic framework of trust modeling and evaluation for ad hoc networks. Selected Areas in Communications, IEEE Journal on, 24(2):305–317, 2006.
[33] M.K.Jeya Kumar, R.S.Rajesh, Performance Analysis of MANET Routing Protocols in Different Mobility Models, IJCSNS International Journal of Computer Science and Network Security, VOL.9 No.2, February 2009
[34] Abdul Hadi Abd Rahman, Zuriati Ahmad Zukarnain, Performance Comparison of AODV, DSDV and I-DSDV Routing Protocols in Mobile Ad Hoc Networks, European Journal of Scientific Research ISSN 1450-216X Vol.31 No.4 (2009), pp.566-576
[35] Dipankar Deb, Srijita Barman Roy, and Nabendu Chaki, LACBER: A new location aided routing protocol for GPS scarce MANET, International Journal of Wireless & Mobile Networks (IJWMN), Vol 1, No 1, August 2009
[36] E.A.Mary Anita, V.Vasudevan, Black Hole Attack on Multicast Routing Protocols, Journal of Convergence Information Technology Volume 4, Number 2, June 2009
[37] Ashwani Kush, P. Gupta and C.Jinshong. Hwang, Secured Routing Scheme for Adhoc Networks, International Journal of Computer Theory and Engineering, Vol. 1, No. 3, August, 2009 1793-8201
[38] Sheenu Sharma, Roopam Gupta, Simulation study of blackhole attack in the mobile ad hoc networks, Journal of Engineering Science and Technology Vol. 4, No. 2 (2009) 243 – 250
[39] Cong Hoan Vu, Adeyinka Soneye, An Analysis of Collaborative Attacks on Mobile Ad hoc Networks, Master Thesis Computer Science Thesis no: MCS-2009:4 June 2009
[40] Irshad Ullah, Shoaib Ur Rehman, Analysis of Black Hole Attack on MANETs Using Different MANET Routing Protocols, Master Thesis Electrical Engineering Thesis no: MEE 10:62 June, 2010
[41] Shishir K. Shandilya, Sunita Sahu, A Trust Based Security Scheme for RREQ Flooding Attack in MANET, International Journal of Computer Applications (0975 – 8887) Volume 5– No.12, August 2010
[42] Akanksha Saini, Harish Kumar, Effect Of Black Hole Attack On AODV Routing Protocol In MANET, IJCST Vol. 1, Iss ue 2, December 2010
[43] Aishwarya Sagar, Anand Ukey, Meenu Chawla, Detection of Packet Dropping Attack Using Improved Acknowledgement Based Scheme in MANET, IJCSI International Journal of Computer Science Issues, Vol. 7, Issue 4, No 1, July 2010
[44] Moitreyee Dasgupta, S. Choudhury, N. Chaki, Routing Misbehavior in Ad Hoc Network, 2010 International

Journal of Computer Applications (0975 - 8887) Volume 1 – No. 18

[45] S. Kannan, T. Maragatham, Attack Detection and prevention methods in Proactive and Reactive Routing protocols, International Business Management 5(3), 2011

[46] Amrit Suman, Praneet Saurabh, Bhupendra Verma, A Behavioral Study of Wormhole Attack in Routing for MANET, International Journal of Computer Applications (0975 – 8887) Volume 26– No.10, July 2011

[47] H. Yang, H. Luo, F. Ye, S. Lu, L. Zhang, "Security in mobile ad hoc networks: challenges and solutions," In proc. IEE Wireless Communication, UCLA, Los Angeles, CA, USA; volume- 11, Page(s):38- 47, ISSN: 1536-1284

[48] Ping Yi, Yue Wu and Futai Zou and Ning Liu, "A Survey on Security in Wireless Mesh Networks", Proceedings of IETE Technical Review, Vol. 27, Issue 1, Jan-Feb 2010.

[49] Y. Hu, A. Perrig, and D. Johnson, "Packet Leashes: A Defense Against Wormhole Attacks in Wireless Ad Hoc Networks," Proc. of IEEE INFORCOM, 2002

[50] K. Sanzgiri, B. Dahill, B.N. Levine, C. Shields, E.M. Belding-Royer, "Secure routing protocol for ad hoc networks," In Proc. of 10th IEEE International Conference on Network Protocols, Dept. of Comput. Sci., California Univ., Santa Barbara, CA, USA. 12-15 Nov. 2002, Page(s): 78- 87, ISSN: 1092-1648.

[51] H. Deng, W. Li, Agrawal, D.P., "Routing security in wireless ad hoc networks," Cincinnati Univ., OH, USA; IEEE Communications Magazine, Oct. 2002, Volume: 40, page(s): 70- 75, ISSN: 0163-6804

[52] D.Suresh kumar, K.Manikandan, M.A.Saleem Durai, Secure On-Demand Routing Protocol for MANET using Genetic Algorithm, International Journal of Computer Applications (0975 – 8887) Volume 19– No.8, April 2011

[53] Zahra Moradi, Mohammad Teshnehlab, Intrusion Detection Model in MANETs using ANNs and ANFIS, 2011 International Conference on Telecommunication Technology and Applications Proc .of CSIT vol.5 (2011) © (2011) IACSIT Press, Singapore

[54] James Cannady, Dynamic Neural Networks In The Detection Of Distributed Attacks In Mobile Ad-Hoc Networks, International Journal of Network Security & Its Application (IJNSA), Vol.2, No.1, January 2010

[55] Nauman Mazhar, Energy Efficient Security in MANET: A comparison of Cryptographic and Artificial Immune System, Pak. J. Engg. & Appl. Sci. Vol. 7, Jul., 2010 (p. 71-94)

[56] Maha Abdelhaq, Rosilah Hassan, Mahamod Ismail, Raed Alsaqour, Daud Israf, Detecting Sleep Deprivation Attack over MANET Using a Danger Theory –Based Algorithm, International Journal on New Computer Architectures and Their Applications (IJNCAA) 1(3): 534-541 The Society of Digital Information and Wireless Communications, 2011 (ISSN: 2220-9085)

[57] Aikaterini Mitrokotsa, Manolis Tsagkaris and Christos Douligeris, Intrusion Detection in Mobile Ad Hoc Networks Using Classification Algorithms, Intrusion Detection in Mobile Ad Hoc Networks Using Classification Algorithms. CoRR, 2008.