Strategic Modelling of Malicious Behavior due to Detour Attack in OLSR Protocol in MANET

Aarohi Surya
Computer Science Department
LNMIIT
Rupa ki Nagal, Post Sumel, via Jamdoli,
Jaipur 302031 Rajasthan
India
aarohisurya@gmail.com

Abstract — Vulnerabilities of Optimized Link State Routing (OLSR) is quite a critical challenge for secure routing system in Mobile Ad hoc Network. Moreover presence of detour attack in OLSR potentially maximizes the threat level. An intruder node performs detour attack by furnishing forged information to its repositories yielding in faulty control message. Therefore, proposed study discusses about a probabilistic technique that can perform modeling of malicious behavior of intruder node under the viewpoint of detour attack using strategic decision making theory or commonly called as game theory. The proposed study designed on cluster uses reputation based factors to map the game theory with detour attacks in MANET. Simulation results are performed in large scale MANET to show the large visualization of unseen and uncertain behaviour of malicious node under the impact of detour attack in MANET.

Key-words; Mobile Ad hoc Network, Detour Attack, game Theory, Malicious Behaviour, Security in MANET

1 INTRODUCTION

A MANET is a collection of mobile devices which are connected by wireless links without the use of any fixed infrastructures or centralized access points [1]. In MANET, each node acts not only as a host but also as a router to forward messages for other nodes that are not within the same direct wireless transmission range. Securing MANET is a highly challenging issue and understanding the possible form of attacks is always the preliminary step towards developing good security solutions. Attacks in MANET are classified as Internal and External Attack where some of the known types of attacks as Denial of Service, Impersonation, Routing Attacks, Black hole attacks, Wormhole attack, Replay attack, Gray- hole attack, etc [2]. Another novel attack which has recently draws attention in security prospect is termed as „detour attack‟ that aims at conserving the attacker's limited device energy by choosing to forward less data packets. A misbehaved node implementing such lethal attack forces a flow to detour around itself by delaying the propagation of routing messages. Hence, the attacker will reduce the possibility of being selected as a forwarding node and could conserve its energy by evading being selected as a router [2]. OLSR is basically table-driven and utilizes an optimization called Multi Point Relaying for controlling traffic flooding [3]. OLSR keeps a variety of repositories in order to maintain state. Information repositories are updated by processing received control messages. Information stored is used to further generate control messages. In OLSR, flooding of control messages is minimized using MPRs. OLSR primly uses HELLO message and Topology Control messages to perform its operation. HELLO messages are broadcast at regular intervals to detect neighbors and the state of the communication lines to them. TC messages describe links between a node and the nodes in its MPR selector set. It was also noticed that OLSR protocol is not even safer in terms of majority of the lethal attacks like detour attacks, black hole attacks in MANET. The neighbors‟ attacking node claims to have, the larger the potential impact of the attack. Therefore, the proposed study presents a solution of lethal attack, specifically, detour attack‟ in MANET against vulnerable OLSR protocol for restricting the attacker(s) to a specific node or a group of nodes from receiving data packets from other nodes who is further than two hops. After investigating the attack in detail, the proposed method will present a simple technique to mitigate the attack. The prime motivation of the current work has been drawn from the study of Rajbir Kaur‟s work „Detour Attack in OLSR‟ [4], where the author have proposed a novel routing disorder attack detour attack against OLSR. In detour attack, a malicious node updates its repositories with fake neighborhood information resulting in generation of incorrect control messages. The fake information forces neighboring nodes to choose the malicious node as their Multi Point Relay (MPR) node. Data packets passing through malicious node are diverted to improper routes and packets may never reach their destination. A large amount of packets sent from source to destination get dropped. In [4], the authors have also analyzed the effects of multiple attackers on network characteristics. The proposed study discusses about the modeling of malicious behavior of the nodes under the vulnerability of detour attack considering OLSR protocol in MANET. Section 2 discusses about the prior research work conducted in mitigating security loopholes in OLSR. Problem identification is discussed in Section 3 followed by proposed system in Section 4. Section 5 discusses about research methodology adopted for current study followed by performance analysis in Section 6. Finally Section 7 summarizes the work discussed in this paper briefly.

2 RELATED WORK

Kannhavong [5] have identified a new routing attack, called Node Isolation attack, against Optimized Link State Routing (OLSR) protocol. The authors have demonstrated the influence of this attack using simulation study. Wang e.t. al [6] have described the security threats to the OLSR MANET routing protocol and presented an intrusion detection solution (IDS) which relies on checking of protocol semantics. While the authors have used OLSR as an example, the authors have argued that the described approach can be applied to any Multi Point Relay (MPR) proactive MANET protocol. Salehi e.t. al [7] have evaluated the effect of different black hole attacks along with various selfish behavior found on the OLSR in MANET. Simulated on NS2, the results shows that such attack highly minimizes routing overhead as compared to basic OLSR. Babu e.t. al [8] have presented an efficient protocol to prevent the collusion attack, by incorporating an information theoretic trust framework in OLSR. This protocol tries to ascertain the presence of the colluding attackers by evaluating and quantifying their trust values based on their uncertainty measures. Hong e.t. al. [9]]have proposed a solution in order to secure OLSR, which uses the technique of wormhole detective mechanism and authentication in order to enhance the neighbor relationship e, and make the use of hash-chain and digital signature verification technique in order to protect the routing packets. Marimuthu and Krishnamurthi [10] have suggested an approach known as enhanced OLSR protocol, an approach based on trust to protect the OLSR nodes against any attack. The experimental results reveal that there is an increase of 45% in the packet delivery while 44% decrement in the packet loss rate, which the protocol is able to achieve, when compared to the standard OLSR. Sadeghi e.t. al. [11] have studied the effects of Wormhole attack on MANET using both OLSR and Reactive AODV. The results have shown that AODV is more sensitive and vulnerable to wormhole attack as compared to OLSR Kruus e.t. al. [12] have presented a detailed description of in-band wormhole in OLSR network. The researchers have identified the independent and continued structures of in-band wormholes and by that presented effective correct measures to protect OLSR. Jeon e.t. al [13] have proposed a protocol named LT-OLSR, which is capable of broadcasting Hello messages to the neighbors in two hops in order to protect the network from the link spoofing attacks. Alam and Chan [14] have focused on the wormhole attack problem in optimized link state routing (OLSR) protocol. The authors have proposed to conduct both round trip time (RTT) measurement and topological comparison to detect wormhole attack. Simulation results show that the method can achieve high detection rate and accuracy of alarms. Kannhavong e.t. al. [15] have presented a collusion attack model against Optimized Link State Routing (OLSR) protocol which is one of the four standard routing protocols for MANETs. The simulation result showed that the attack can have a devastating impact on the OLSR MANET. After analyzing the attack, we have presented a simple mechanism to detect the attack by adding the address of 2-hop neighbors in HELLO message.

3 PROBLEM IDENTIFICATION

In this section we discuss various security vulnerabilities in OLSR. In OLSR, each node has two different responsibilities – (i) to generate correct routing protocol control traffic according to protocol specification, (ii) to forward routing control traffic on behalf of other nodes present in the network. Intruder behavior of a node can result in generation of incorrect control messages or incorrect relay of control messages. There is no mechanism in OLSR to validate correctness of information sent by a node to its neighbors. Neighbor nodes process and forward all information even if it is generated by an intruder node. This may cause various problems in the network. In the following section we propose a novel attack model where an intruder node exploits the vulnerabilities inherent in OLSR to cause routing misbehavior. A misbehaving node can disrupt the integrity of the network by either incorrectly generating or relaying control traffic information on behalf of other nodes. The selfish behavior of the node can be seen when the attack is performed by a node that misbehaves and neither generates nor forwards TC messages. To increase the effectiveness of the attack, the intruder node might establish false links to other nodes in the network and force its one-hop neighbors to select it as their MPR.

4 PROPOSED SYSTEM

The proposed work targets to address the issues of detour attack in mobile ad hoc network specifically targeting OLSR protocol. In order to accomplish this goal, following are the research objectives:

- To propose a security framework that can potentially understand the behavior of the misbehaved node in OLSR protocol in MANET.
- To design a framework that can be efficiently used to model the uncertain behavior of the misbehaved nodes in MANET.

Although there is considerable amount of work done in security of the routing protocols on mobile ad hoc network as seen in review of literature, but the proposed system gives higher contrast result compared to all major previous work by considering the probabilistic approach of identifying the routing behavior of the intruder node as an outcome of detour attack in MANET. One of the most significant criteria considered for the proposed system is analyzing and distinguishing the behavior of either normal node or the intruder node. The simulation of the proposed system will consider virtual competition for representing the implications of respective roles of individual actions for normal nodes and intruder nodes. In this proposed approach of virtual competition, the mobile nodes will scrutinize the results of each specific communication occurring. In the experiment, each mobile node will design a reputation factor towards its neighboring nodes and update their reputation information in accordance to the neighbor's actions as the virtual competition evolves.

The flow diagram of the proposed study is shown in Fig.1. Prior researches in this field has not succeeded to consider the feasibility that an intruder might select different threat frequencies toward different opponents whereas the proposed project work considers more "Smart" intruder nodes, making the normal and intruder nodes‟ competition in this proposed model more realistic. This is the reason of deploying the proposed algorithm.

The proposed research work is basically based on mathematical modeling and therefore the research questions of the proposed study should relate to mathematical attributed associated with the study that are as follows:

□ How to estimate the belief system of MANET considering the presence of regular, selfish, as well as malicious nodes?

□ What procedure can be adopted to compute the uncertainty in the decision adopted by the mobile nodes?

□ How to simulate the multiple behaviors of various nodes considering the unpredictable situation of next strategies to be adopted by the mobile node?

□ How to model the probability of unique strategies being adopted by multiple attacker nodes present simultaneously in n-number of clusters?

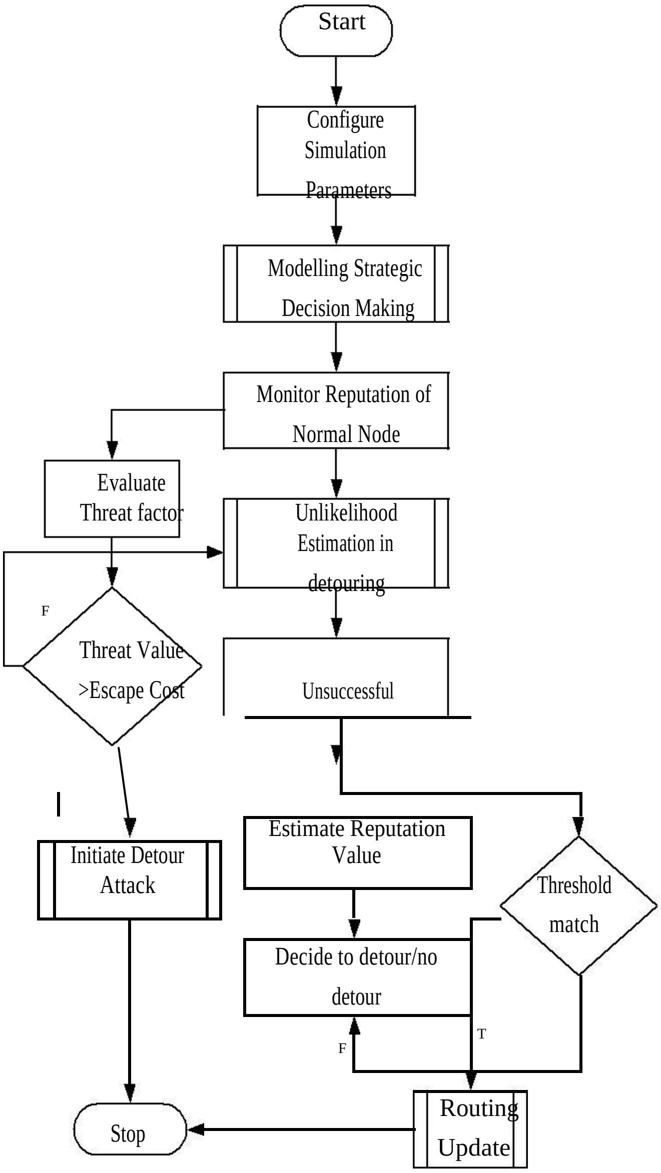
Start
Configure Simulation Parameters
Modelling Strategic Decision Making
Monitor Reputation of Normal Node
Evaluate Threat factor
Unlikelihood Estimation in detouring
F
Threat Value >Escape Cost
Unsuccessful
Initiate Detour Attack
Estimate Reputation Value
Threshold match
Decide to detour/no detour
F
T
Stop
Routing Update

Figure 1 Flow of the Proposed Model

5 RESEARCH METHODOLOGY

The proposed study introduces basically an attack model that exploits flaws in OLSR in MANET specifically termed as detour attack. In the proposed attack model, a misbehaving node updates its link table with incorrect neighborhood information. Erroneous neighborhood information disseminates in the network. Inaccurate routing tables are generated. Packets intended for destination do not reach it, resulting in packets being dropped. The proposed research methodology is classified into 4 phases:

1. This is the preliminary phase that intends to gather all the information related to various types of attacks on MANET, mis-behaviour of nodes, diversion issues created in routing, and more related works on detour attacks in MANET.

2. This phase primly investigated various standard and efficient techniques that were implemented in past for securing various attacks on OLSR protocol in MANET. The study will yield to arrival of solution that could be possible adopted in the proposed study governing detour attack in MANET.
3. This is one of the core phases of the research methodology which mainly targets to model the misbehavior of the nodes in MANET. This phase basically intends to understand and model various uncertain behaviors of mis-behaved nodes in MANET, so that a new model can be designed for formulating the strategies of mis-behaved nodes. An adversarial module will be designed in this phase that will mainly perform collection of network information, updating own topology information, and broadcast forged information to the neighbor nodes. Finally, a probabilistic model is planned to design that should address the issue of visualizing the patterns of behavior of mis-behaved nodes in MANET.
4. The framework created in previous will be now extended for modelling detour attacks in MANET by introducing a novel network model using cost effective cryptographic approach. It is expected that accomplishment of this phase will render the cumulative model to understand the behavioral pattern as well as to mitigate the threats of detours attack in OLSR in MANET.

The proposed system analyzes the mobile ad hoc network to identify the optimal decision protocols and events by deploying the framework which chooses to achieve perfect Bayesian Equilibrium.

The proposed contribution for the study is to represent the normal / intruder node with virtual competition as a multi phase scheme to find the optimal policy of normal and intruder nodes for computing the general decision process of normal and intruder mobile nodes in case of detour attack in MANET. The proposed system also observes a threshold schema to choose whether to update other mobile nodes in the logical region or not. If not the normal node chooses to assist with the probability which is estimated depending on the reputation level. Not only this, the intruder node also estimates the threat of being caught in its existing location, so it follows its protocol to decide whether it should decamp to another logical region or not. If not, the intruder mobile node will choose to attack. The prime issue in this decision process is the decision rules for both normal and intruder nodes and the event profiles shown by the probability that the normal node cooperates and the probability that the intruder node attacks.

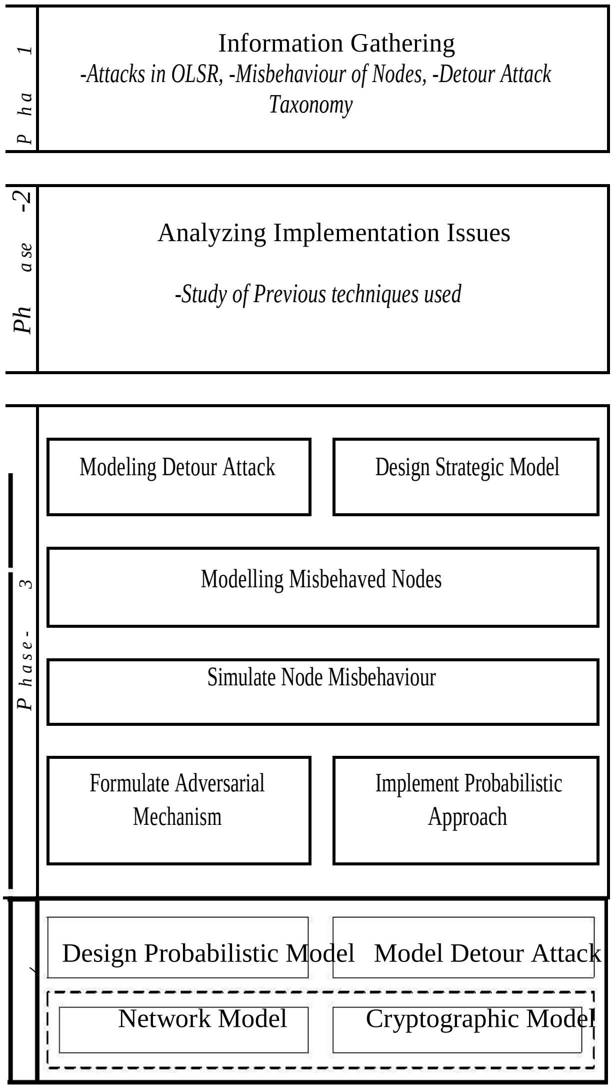
P ha 1
Information Gathering
-Attacks in OLSR, -Misbehaviour of Nodes, -Detour Attack Taxonomy
Ph ase -2
Analyzing Implementation Issues
-Study of Previous techniques used
P hase- 3
Modeling Detour Attack
Design Strategic Model
Modelling Misbehaved Nodes
Simulate Node Misbehaviour
Formulate Adversarial Mechanism
Implement Probabilistic Approach
Design Probabilistic Model
Model Detour Attack
Network Model
Cryptographic Model

Figure 2 Illustration of Implementation Strategy.

The algorithms deployed are discussed

below.

Algorithm-1: Communication Model

Objective: The main objective of this algorithm is to estimate all the parameters (nodes, velocity of node, length and width etc) and it also assigns the new positions for the movement of the nodes from its old position.

Input: x-node, y-node, speed, length and width

Output: The program estimates all the parameters responsible for the communication and mobility model of MANET.

STEPS:

```
1 Initialize x-node, y-node, speed, length
and width 2 create a function for calculating
parameters
3 Calculate first random position (r1) for the
node to travel
4 Calculate second random position (r2) for the
node to travel
5 Estimate new position of x-node (x-new)
6 Estimate new position of y-
node (y-new)
7 If (x-new<0 || x-new>length)
8 Assign (x-node-r1) to x-new
9End
10 If (y-new<0 || y-new>width)
11      Assign (y-node-r2) to y-new
12End
```

Algorithm-2: Estimating Probability of Intruder Node in detouring.

Objective: The main objective of the algorithm is to estimate the probability of intruder node in the MANET environment.

Input: Xc and Ya

Output: Calculation of the probability of intruder node invoking detouring.

Steps:

```
1 Initialize number of detected cooperation (Xc)
2 Initialize numbers of detected attacks (Ya)
3 Create a function for estimating probability of
intruder node.
4 Initialize probabilities that the node is an intruder
node (Pm) 5 Apply Formula:
```

$Pm = Ya / (Xc + Ya)$

Algorithm-3: Estimating Reputation Factor

Objective: The main objective of the algorithm is to estimate the reputation factor by considering number of detection cooperation, attacks, and improbability in the vulnerable environment of MANET due to detour attacks.

Input: Xc, Ya, Uo

Output: The program evaluates the reputation factor

Steps:

1 Initialize number of detected cooperation (Xc)

2 Initialize numbers of detected attacks or declines (Ya)

3 Initialize unlikelihood in the opinion (Uo)

4 Create a function for calculating the reputation system

5 Initialize temp_var1 and temp_var2

6 Assign (Xc/(Xc + Ya)) to temp_var1

7 Assign (1-Uo) to temp_var2

8 Estimate reputation Factor (Rept) in the opinion by applying formula

Rept = temp_var1+temp_var2

9 Show the detoured links.

Algorithm-4: Calculating unlikelihood of opinion for detour attack detection

Objective: The main objective of the algorithm is to estimate the unlikelihood

Input: Xc, Ya, Uo

Output: The program gives the estimation of unlikelihood factor for detour attack detection.

Steps:

1 Initialize number of detected cooperation (Xc)

2 Initialize number of detected attacks (Ya)

3 Create a function for estimating unlikelihood

4 Estimate unlikelihood in the opinion (Uo) by formula: $Uo = 12 \text{ x } Xc \text{ x } Ya / \{(Xc + Ya)^2 \text{ x}(Xc+Ya+1)\}$

6 PERFORMANCE ANALYSIS

The proposed system has studied a large field of policies of intrusion in dynamically produced MANET (mobile ad hoc network) in Matlab platform. The regular node is considered to follow its respective neighboring transmitted message by neighbor monitoring. A simulation framework of 1000 x 1000 m is designed with 200 mobile randomly positioned with a transmission range of 300 meters. A mobility model is designed and any two nodes in the same cluster are considered as neighboring nodes.

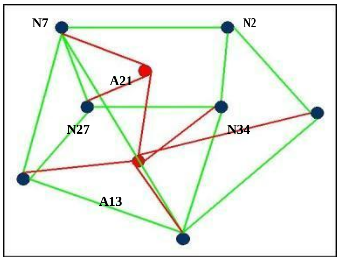

Figure 3- Unit Cluster showing 7 normal node and 2 intruder node.

Fig 3 represents an instance of simulation where 200 mobile nodes are randomly distributed in nine logical regions. The red colored line shows the communication between two mobile nodes in the same logical region. The blue colored line represents probable communication link between two mobile nodes in the same logical region.

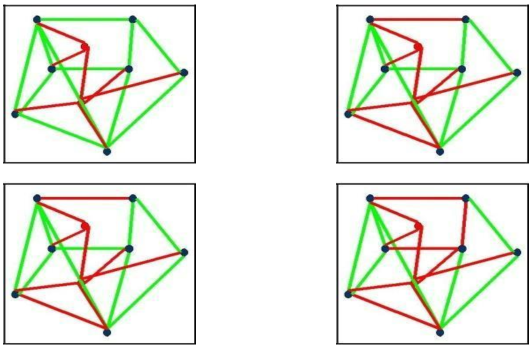

Figure 4- 4 clusters regions with 28 regular nodes and 8 intruder node with detouring (Red lines).

In figure 4, the process of decamping is depicted by green colored lines from the attack region to a new logical region. The analysis is carried out by checking the consequences of various phases of the virtual competition to explain the anomalous nature of the nodes.

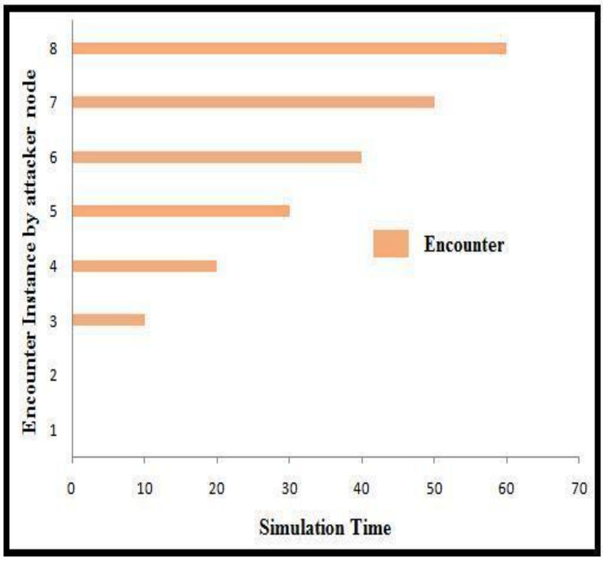

Figure 5- Analysis of Encounter of attack nodes with Regular node

Fig-5 represents encounter of attack nodes with normal nodes. The graph represents very uneven variation proving difficult to predict the encountering strategy of attack nodes in the MANET environment.

Figure 6 represents that with every attempt of attack, the countermeasures provided to update the attack information to the other cluster increase, which shows the robustness of the proposed methodology.

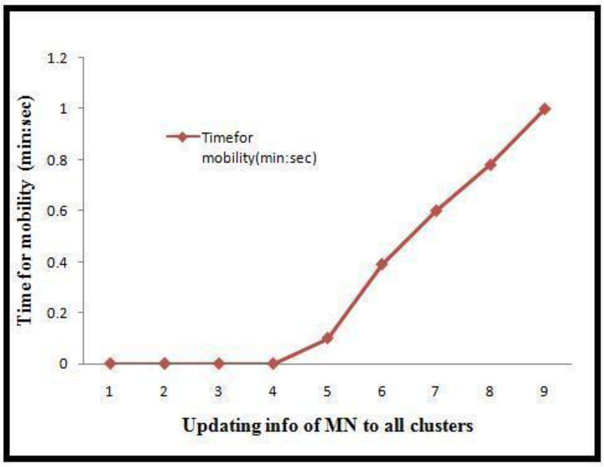

Figure 6- Cluster updates during attack by intruder nodes

One of the main attempts of the proposed system is to understand the misbehavior of the nodes in the MANET environment. In real-time scenario, it is almost difficult task to estimate time of the attack probability, which pose a great threat to the existing cluster as well as neighborhood clusters. So the figure 7 represents that with every node-to-node communication, there is a peak seen representing highest attack probability. This also represents that it is highly possible to understand the attack strategy if the simulation parameters are kept on changes based on multi-stages according to game theory.

7 CONCLUSION

The proposed system discusses about the modelling of malicious behavior of the node under the circumstances of detour attack. The outcome of the proposed model are as follows-i) A robust behavioral analyzer is design that has accomplished in a probabilistic model for empirically modeling the misbehavior pattern of the detour attack in OLSR in MANET. ii) An efficient and scalable mitigation techniques is designed that addresses large scale mobile ad hoc network considering both single and multiple attacker considering detour attacks on OLSR in MANET, and iii) Computationally cost effectiveness is accomplished where the proposed system is a simple model and independent of any cryptographic technique that addresses detour attacks potentially with scalable performance measures on QoS using game theory. The current study has identified some of the computationally challenging task pertaining to the security aspects of mobile ad hoc network using game theory to analyze the behavioral pattern of various nodes in mobile ad hoc network. The system can illustrate the rationale behind the node's adopted behavior considering both regular as well as malicious node.

REFERENCES

[1] Yi, J., A Survey on the Applications of MANET, technical Report, 2008

[2] Rai, A.K., Tewari, R.R., Different Types of Attacks on Integrated MANET-Internet Communication, International Journal of Computer Science and Security, Volume (4): Issue (3), 2012

[3] Jacquet, P., Muhlethaler, P. ; Clausen, T. ; Laouiti, A., Optimized link state routing protocol for ad hoc networks, IEEE, 2001

[4] Kaur, R., Kumar, M., Laxmi, V., Gaur, M.S., Detour Attack in OLSR, ACM, 2011

[5] Kannhavong, B., Nakayama, H., Jamalipour, Analysis of the Node Isolation Attack Against OLSR-based Mobile Ad Hoc Networks, IEEE 2006

[6] Wang, M., Lamont,L., An Effective Intrusion Detection Approach for OLSR MANET Protocol, IEEE 2005

[7] Salehi, M., Samavati, H., Dehghan, M., Performance

Assessment of OLSR Protocol under Routing Attacks, IEEE 2011

[8] Babu, M.N., Franklin, A.A., Murthy, S.R., On the Prevention of Collusion Attack in OLSR-based Mobile Ad hoc Networks, IEEE 2008

[9] Hong, F., Hong, L., Fu, C., Secure OLSR, IEEE 2005

[10] Marimuthu, M., Krishnamurthi, I., Enhanced OLSR for Defense against DOS Attack in Ad Hoc Networks, Journal of communications and networks, Vol. 15, no. 1, February 2013

[11] Sadeghi, M., Analysis of Wormhole Attack on MANETs Using Different MANET Routing Protocols, IEEE 2012

[12] Kruus, P., In-Band Wormholes and Countermeasures in OLSR Networks, IEEE 2006

[13] Jeon, Y., Kim, T.H., LT-OLSR: Attack-Tolerant OLSR Against Link Spoofing, IEEE 2012

[14] Alam,M., Chan, K.S., Topological Comparison Based Approach of Detecting Wormhole Attacks in OLSR Protocol, IEEE 2010

[15] Kannhavong,B., A Collusion Attack Against OLSR-based Mobile Ad Hoc Networks, IEEE 2006