Journal of Theoretical and Applied Information Technology
20th February 2014. Vol. 60 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

# THE IMPACT OF LOCATION BASED ATTACKS ON GEOGRAPHICAL ROUTING PROTOCOLS

**[1]B.MUTHUSENTHIL, [2] S.MURUGAVALLI**

[1]Assistant Professor., Department of Computer Science and Engineering,
Valliammai Engineering College, Chennai
[2] Professor & Head., Department of Computer Science and Engineering,
Panimalar Engineering College, Chennai
E-mail: [1]bmssen@gmail.com, [2]murugavalli26@rediffmail.com

**ABSTRACT**

Several applications of mobile ad hoc networks select geographical routing especially the Greedy Perimeter Stateless Routing (GPSR) protocol due to its scalability, efficiency, and ability to support location based applications. However, there are many security issues in protecting location information, which can easily be abused by attackers. Location based adversarial activities affect the operation and performance of geographical routing protocols. There are only a few works on the literature that studied the impact of location based attacks on geographical routing. This work analyzes the impact of malicious nodes on the GPSR performance associated with fake location. This proposal identifies a set of possible location based attacks and analyzes the local problems that arise from the location based adversarial activities. Finally, it demonstrates the overall impact on the routing performance, by simulating the network in various attack scenarios. This study illustrates the effect of the adversarial activities with respect to the packet delivery ratio, overhead, average end-to-end delay, routing loops, packet dropping probability, and location error rate. The simulation results concluded that the overall routing performance degrades, depending on the type and percentage of adversaries.

**Keywords:** *Location Based Routing, Location Information, Active Attack, Passive Attack, And Impacts*.

## 1. INTRODUCTION

The location based routing in Mobile Ad Hoc Networks (MANETs) has emerged as an interesting area of research over the last few years. Location based routing protocols in MANET use the physical location of the nodes to forward the packets. Some of the geographic routing protocols are GPSR [1], Distance Routing Effect Algorithm for Mobility (DREAM) [2], Location-aided routing (LAR) [3], Directional Antenna Multi-path Location Aided Routing (DA-MLAR) [4] and GRID [5]. This work focuses mainly on the GPSR protocol, but it appears to be derived from [6]. A survey of geographic routing protocols has been provided in [7] and [8]. The exploitation of physical locations of the nodes can significantly enhance their routing efficiency and scalability for the mobile ad hoc networks. This results in greatly reducing the routing overhead and provides a better packet delivery rate. The geographic routing protocol does not involve in distributing the control packets over the entire network. The geographic routing protocol is more feasible for large scale network [9]. Moreover, the location based routing requires only low memory.

In the GPSR, the nodes periodically broadcast their position through beacons so that nodes within the transmission range can construct the table of neighborhood list along their position. Each node in geographic routing obtains the location information using the Global Positioning System (GPS) [10] [11] [12]. In geographical routing, a node forwards the packet to its next hop that is closest to the destination. The most common technique for the forwarding packet in geographical routing is greedy forwarding. In location-based routing, every node retains its own location information at more than one location server. Each node queries the location server to attain the destination‟s location for communicating with the destination. The location server replies to the node if it has the appropriate location information. In the geographical routing, it is noticed that the packet delivery ratio gets reduced with the average error in location information.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

If the location information is available, the location based routing is appealing as it is easy to perform and is scalable. Most of the existing works on location based routing have assumed that the location information obtained at each node is faultless. But, practically, only a rough approximation of the location information is available. If a node reports wrong positions, the routing process gets influenced. The wrong position statement may be due to improper functioning of the positioning hardware or may be the adversaries intentionally falsify the route information to reroute the data packet. The presence of adversaries degrades the performance of a network to some extent. Any adversary in the network is capable of degrading the network performance. The location information based attackers have ability to launch the attack despite strong detection mechanisms. The adversaries can even increase the false alarm rate. This work attempts to prove that the faulty location information announced by the adversaries" results in performance degradation of location based routing. This work also attempts to report on the impact of the location based attacks over the network performance.

### 1.1 Contributions

The major contributions of this work include:

- Initially identifies a set of attacks that targets location information, time and distance information in GPSR and investigates the interruptions or problems caused by the location based attacks.
- Analyzes the impacts of active and passive attacks on the GPSR"s performance in terms of routing metrics such as packet delivery ratio, routing overhead, average end to end delay, routing loops, packet dropping probability and location error rate.
- Finally, it analyzes the reasons for performance degradation and estimates the level of performance degradation of the GPSR in the presence of 40% of the attacks.

### 1.2 Paper organization

The remaining sections of this paper are organized as follows: Section 2 lists out the feasible attacks in location based routing and classify them. Section 3 analyzes the impact of the location based routing attacks over the routing process. The first fold of section 4 discusses the simulation scenario and performance metrics. The second fold of section 4 deals with the performance evaluation of the impacts of the location based attacks over the network performance. Section 5 concludes the paper.

## 2. FEASIBLE ATTACKS IN LOCATION BASED ROUTING

In the past, several geographical routing protocols have been suggested that follow greedy forwarding and recovery procedure. GPSR is the most widely used geographical routing protocol that uses perimeter or face routing to avoid voids if greedy routing fails. On the other hand, geographic routing protocols are vulnerable to location based attackers. Previous works have analyzed that location based attackers can result in performance degradation in a large level [13] [14]. The performances are mainly analyzed in terms of packet delivery ratio, overhead and delay. Geographic routing protocols are stateless in nature. Each node maintains the location information of its one-hop neighbors. Location based routing have several advantage over topological routing. Location based routing protocols are much suitable for large scale networks. The nodes use low memory as they store only local information. The major components of location based routing include location service and geographic forwarding process. The Location service provides the location of the destination node if the source node queries it. The location of the destination is added to the packet header, thus helping the intermediate nodes to identify the packet"s end host. This location information can be easily accessed by adversaries as geographic routing does not meet the security requirements. The location services are also vulnerable to attacks and the work in [15] analyzes the attacks on location services.

This work attempts to identify the feasible attacks based on the information location and location services and to prove that the location based adversaries create certain impacts on the network performance. There are some location based attacks against geographic routing protocols as discussed below. In the mobility attack, the adversaries move to a new location after obtaining a valid location certificate [16]. This adversary makes use of the validated location information that is no longer

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

valid. This attack is much difficult for location verification techniques to detect as it maintains the correct location during the location verification. The impact of mobility attack can be reduced by frequently requesting fresh location verification certificates if communicating with a neighbor for the first time. This attack causes a large amount of additional overhead.

In the multi query attack, the actual location of the service requester can be inferred by the adversary through obtaining cloaking regions that are minimized or enlarged in consequent queries [17]. The adversaries launch the multi query attacks by compromising the actual physical location of the query distributor with the aid of several spatial queries that have different cloaking regions. The multi query attack can be described in two forms such as shrink region and region intersection attack.

Selective forwarding attack selectively forwards a small number of packets instead of dropping all the packets. These adversaries cannot be detected easily, and they have an alternative route through which packets can be forwarded. Selective forwarding attack causes considerable packet loss. The advanced adversary targets the localization process. Localization in the geographic routing is based on parameters like Received Signal Strength (RSS), Time Difference of Arrival (TDOA), Time of Arrival (TOA), and hop count [18]. These factors depend on the physical properties of the wireless medium. Adversaries can launch non cryptographic attacks against these parameter measurement processes, and hence, degrades the localization performance. For instance, the attenuation attack decreases the transmission range and hence, increases the number of hops between the source and the destination. The compromised nodes delay the reply packets to disrupt the time and distance determination. The adversaries can even attenuate or amplify the signal strength, thus altering the RSS readings.

## 3. SYSTEM AND ATTACK MODEL

The communication network is represented as a graph G= (V, E), where V is a group of nodes and E is a set of edges between them. An edge (P, Q)∈E represents a direct connection between two nodes P and Q, which means Q is in the communication range (CR) of P, and vice versa. In this case, P and Q are said to be neighbors and N (P) represent the neighbor set of P.

$$E(P, Q) = \{Q, Q \in N(P) \wedge (P, Q) \in V\}$$

The geographical routing is mainly based on the position information. In GPSR, the greedy node (VG ∈ N(P)) is selected on the basis of node P"s location information and Distance between the VG and destination (VD), δ(G-D). Let P (x, y) be the position of P ∈ V. Each node P ∈ V is equipped with the GPS receiver that enables them to gather P (x, y). The condition for selecting VG in terms of distance is as follows:

$$\delta G\text{-}D < \forall\{[\delta N(P) - D] - [VG \in N(P)]\}$$

V comprise of both legitimate (VL) and attacker (VA) nodes such that V= (VL, VA). This work considers about 40% of VA∈V. Let D is the diameter of the total network. Let VA/P be the probability of attackers to attack a node P when selecting its greedy node.

$$VA/P \in CR(P) = \{0.04CR2\}/D2$$

The attack nodes VA/P∈ CR (P) may attack the communication between P∈V and VG in active and passive. In active attack, the VA/P modifies the parameters including P(X,Y) and δ(G-D) that are involved in the VG selection. In passive attack, VA/P just monitors the beacon packet parameters such as timestamp and distance metrics to launch pinpoint attack.

## 4. CLASSIFICATION OF ATTACKS ON THE GPSR

The common location based attacks are discussed in this section with their impacts on the routing performance. The attacks on the GPSR can be broadly classified into two categories namely, active and passive attacks. Both the active and passive adversaries can launch numerous attacks against the GPSR. These attacks are further classified as follows.

Journal of Theoretical and Applied Information Technology
20th February 2014. Vol. 60 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

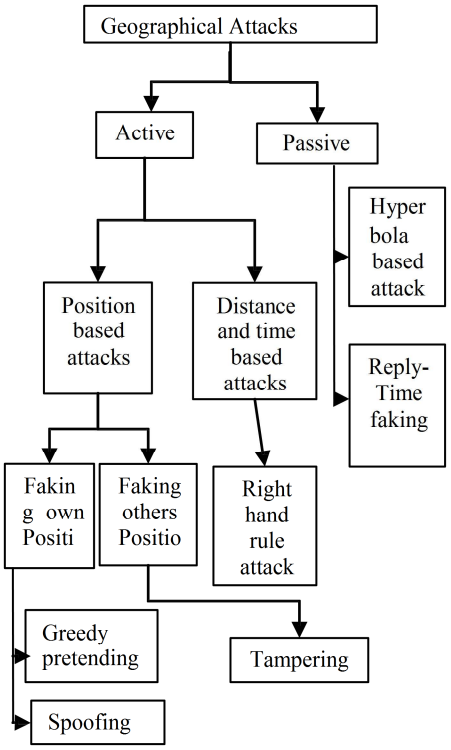


*Figure 1: Classification of Attacks in GPSR*

### 4.1 Active Attacks

The active attacks access the information in the messages to disrupt the communication operation. An active attack modifies the information of packets, and impersonates other nodes. The active attacks can be further classified on the basis of position, and distance and time.

#### 4.1.1.1 Faking own position

The attackers launch an attack by faking their own positions. The attacker"s gains the traffic by faking its own position and does not fake an others position [19].

#### 4.1.1.1.1 Greedy pretending

Figure 2 demonstrates a scenario in which node M pretends to be at position m. According to the greedy forwarding scheme, the node S selects A as the next greedy (forwarding) node that is the one closest to the destination. The node A will then forward the packet to the next nearest node to the destination. The actual greedy node for node A is node M, but adversary M provides a fake position m instead of providing its real position. Therefore, node A selects m as its greedy node and forwards the packet. Therefore, the packet ends at node M that can either forward or drop it.

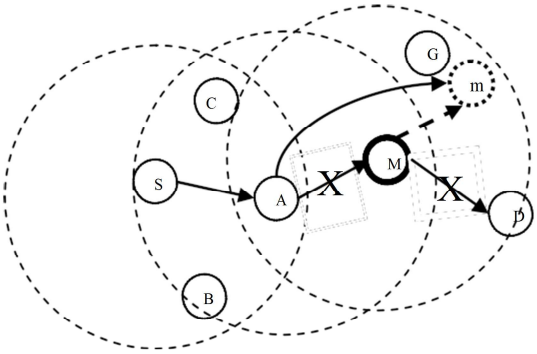


*Figure 2: Greedy pretending*

#### 4.1.1.1.2 Greedy Spoofing

A non greedy node spoofs the position of the greedy node and it sends the reply beacon using the spoofed position with the latest timestamp after the actual greedy node"s reply. This attack does not drop any packet but results in denial of service.

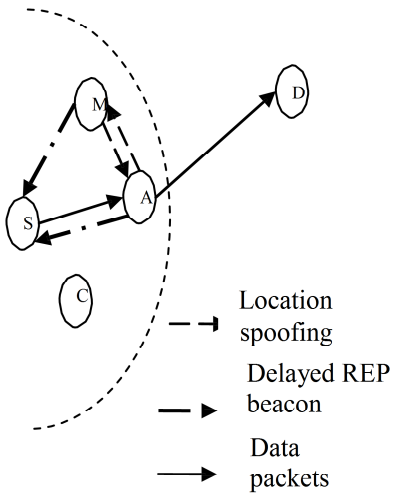


*Figure 3: Greedy Spoofing*

Figure 3 shows the greedy spoofing attack in which the node M spoofs the location of greedy node A and waits till node A sends reply for beacon message to S. The node M sends the reply to node S with the delay of d' i.e. greater

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

than the actual delay d from node A to S. This attack causes denial of service degrading the routing performance of the GPSR. Table 1 shows the actual delay and the delay introduced by the adversary node M using the spoofed location of node A.

| Actual (from A) | | Spoofed (from M) | |
|---|---|---|---|
| Location | Delay | Location | Delay |
| $(X_A, Y_A)$ | d | $(X_A, Y_A)$ | d + d' |

*Table 1: Information in REPLY beacon messages*

**4.1.1.2 Faking an others position**

The attackers launch an attack by faking an others position. These attackers fake the other node"s position in the location information and forward the packet with the modified location information.

**4.1.1.2.1 Tampering attack**

In the location based the routing, the forwarding decision by a node is based on the location information it receives. Adversaries can modify the location information in messages intentionally to interrupt the geographic forwarding strategy. This attack is called location information tampering attack [20].

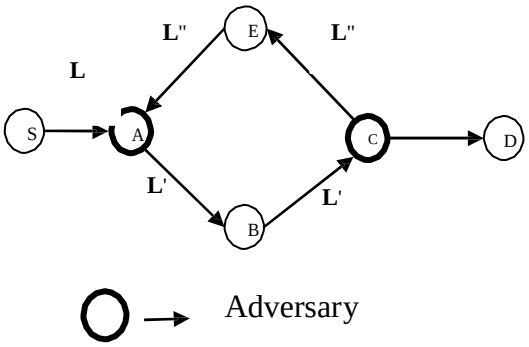


*Figure 4: Location information tampering attack*

In figure 4, there are two paths between S and D such as S-A-E-C-D and S-A-B-C-D. If a node „A" receives a message L from S, it can alter the location information of D and forward the altered message L' to other colluding node C through node B. If node B receives L', it re-modifies the message as L" and forwards to A again through node E. This results in the formation of routing loop in which the location information passes nodes in a cyclic manner without being routed to the original destination D.

**4.1.2 Distance and Time Based Attacks**

In geographic routing, the greedy nodes are selected based on distance and time. The beacon packet includes the details of distance and time during the greedy node selection. The adversaries can modify this information to degrade the GPSR performance.

**4.1.2.1 Right Hand Rule Attack**

In the greedy forwarding, it is impossible for a node to have a neighbor closer to the destination than itself; this result in formation of void. In this scenario, the greedy mode of routing fails and switches to perimeter mode. The perimeter mode employs the right hand rule to eliminate the crossing nodes [1]. An adversary in GPSR attacks not only the greedy mode but also the perimeter mode. The right hand rule states that if a void node A receives packet from node B, the node A selects its neighbor that is counterclockwise about itself from edge AB.

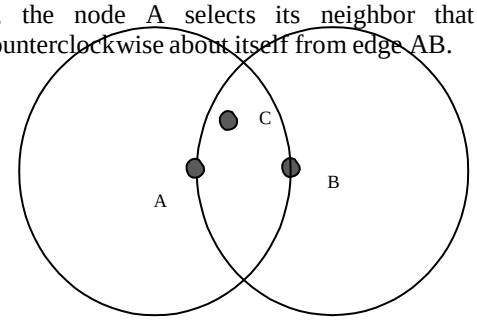


*Figure 5: Right hand rule- Perimeter*

An edge (A, B) exists between vertices A and B if the distance between them $D_{A,B}$ is less than or equal to the distance between all other vertex C and any of A and B is away from C. It can be expressed as:

$$\forall C \neq A, B: D_{A,B} \leq \max [D_{A,C}, D_{B,C}]$$

The attackers can launch attack on the distance metrics to delay the data forwarding under perimeter routing and it is called right hand rule attack. In the figure 5, the attacker C

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

disrupts the perimeter mode by stating that the total distance of $D_{A,C}$ and $D_{B,C}$ is lesser than $D_{A,B}$

### 4.2 Passive Attacks

A passive attack does not modify the information in the messages. A passive attacker has ability to launch several attacks even in the presence of strong detection mechanisms.

#### 4.2.1 Reply- Time faking

The adversary node does not send a REPLY as soon as it receives the beacon packet. Instead, it waits for actual greedy node to send the REPLY and later it sends REPLY with the recent timestamp [19].

#### 4.2.2 Hyperbola Based Attack

The hyperbola based attack is a passive attack as it monitors the beacon reply time of the greedy node to create the fake position on the hyperbola with respect to the sender and the greedy node [19]. If the adversary node M is aware of A‟s position information ($A_{X,Y}$), it announce the fake position that on the hyperbola with respect to the node S and it advertise the delay of $T'_M$ in its beacon reply. It is difficult to determine when it takes the position information, m on the hyperbola with the knowledge of the accurate delay.

$$T'_M = T_A + [(A_{X,Y})-(M_{X,Y})]/V - [(A_{X,Y})-(m_{X,Y})]/V$$

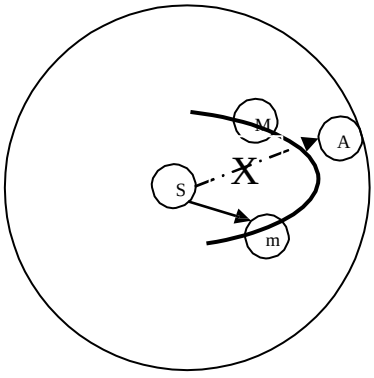


*Figure 6: Hyperbola Based Attacks*

## 5. IMPACTS OF ATTACKS ON GPSR PERFORMANCE

This section analyzes the impact of various attacks on the performance of the GPSR.

### 5.1 Impacts of position based attacks

If a node‟s actual position is not in the route between the source and destination and neither is the fake position, then there is no impact of adversaries on the system performance. If the actual and fake positions are in the route between source and destination and position in the specified route does not change, there is no impact of adversaries on the system performance.

The following cases have more impact over the network performances.

One of the major impacts of position faking on GPSR performance is the increasing average end to end delay. If a node does not able to receive the packet as a result of position faking attack and if the routing protocol recognizes the packet loss using acknowledgement or timeout techniques, the packet may still be delivered to the destination with the aid of some back-up strategies. This process will introduce extra delay and reduce the available bandwidth. If the routing protocol does not adopt any back-up strategy, the data packets get lost. Transmitting a data packet several times before it reaches the destination results in a considerable average end to end delay.

If the actual location of the node is far away from the destination than the fake location and the node may forward the packet such that it reaches the fake location again. This adversarial activity leads to routing loops. The routing loop occurs till the packet‟s time-to-live expires.

As discussed above, location faking attack is a serious issue that affects the system performance, reliability and security of the ad hoc network with location based routing.

### 5.2 Impacts of distance and time based attacks

The greedy failure in the local maximum is one of the most important problems in the GPSR. Distance is the main metric that decides the forwarding node in the perimeter mode and the adversary targets this information to launch attacks. The inaccurate distance information provided by the adversary increases the packet

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

drop. The dropping of data packets leads to redundant re- transmission, thus, increasing the average end-to-end delay. The adversaries select one of the previous senders in the routing path and forward the packet resulting in a loop. This kind of adversaries increases the path length or hop count resulting in additional delay. The performance of geographic routing protocol in terms of packet delivery ratio, control overhead, and average end-to-end delay varies with the percentage of attackers.

### 5.3 Impacts of passive attacks

In the REPLY time faking attack, the adversary node monitors the greedy node‟s REPLY time and sends the REPLY beacon after the REPLY of actual greedy node to become greedy node. This adversarial activity results in denial of service. In hyperbola attack, the adversary nodes should have all the knowledge about the source and greedy node including the location and distance exactly to fake its position on the hyperbola of source and greedy node. This process increases the overhead in the GPSR performance. If there is a node in the claimed fake position, the packet is either dropped or delayed at will. The adversary in passive attacks leads to a non-optimal greedy selection which in turn leads to an increase in hop count. It drops the packets if the TTL of the packet gets expired. Both these actions degrade the network performance in terms of delivery ratio and average end to end delay.

## 6. SIMULATION ANALYSIS

This section deals with the simulation of the geographical routing protocol in the presence of attackers and analyzes the simulation results.

### 6.1 Simulation scenario

The ns-2 simulation model is used to analyze the impact of adversaries on the ad hoc network with the geographic routing protocol. For simulating the impact of location based attacks on geographic routing, this work selects GPSR as the routing protocol. In location based routing, this network scenario considers greedy forwarding approach for forwarding the packets. The ns2 simulation is performed for 150 nodes that are equally distributed in the density of 0.00015 over the region of 1000 m X 1000 m, with the nominal 250 m communication range. For simulation purposes, 40% of the total nodes are considered as attackers. The nodes follows the random way point mobility model with the velocity of 10 m/s. The pause time for each node is 75 seconds. The simulation lasts for 150 seconds of simulated period.

#### 5.3.1 Attack model for simulation

The autonomous network is represented as a directed graph G (V, E) in which V represents the nodes/ entities and E represents the edges. Let „N‟ represent the total number of nodes in the network such that |V|= N. The network scenario is considered with the presence of a certain percentage of malicious nodes. The malicious nodes select a random location for advertising its fake position using a beacon message. Moreover, if the malicious node receives a packet, based on the simulation set-up, it may either forward or drop the packet. Let $A_A$, and $A_P$ represent the active and passive adversaries. $A_A$ has the ability to modify the contents in the messages whereas $A_P$ launches attacks by just monitoring the communication traffic. The $A_A$ comprises the position based attackers ($A_F$) and distance based attackers ($D_F$). 40% of the attackers from each type of attack are considered for simulation. Based on the attacks considered i.e. active and passive, they can be modeled as follows:

Let T(x, y) be the original position of T$\in$ $A_A$. T launches position faking attack by reporting a false position $\check{T}$ (x, y) $\neq$ T (x, y). Let nodes P and Q be the one hop neighbors of T. The reported fake position $\check{T}$ (x, y) can alter the one hop relationship of the nodes P and Q.

Let TD be the original delay of beacon reply of T. The node T monitors the delay time of original greedy node (G), $G_D$. Then T $\in$ $A_P$ sends the reply with a delay of $T_{D+D'}$.

### 6.2 Parameter metrics

*Packet delivery ratio:* It is the ratio between the number of data packets received by the destination and the number of data packets transmitted by the source.
*Routing overhead:* It is the total number of bytes of control packets involved in the routing
*Average end-to-end delay:* It is the time between the origination of the packets from the source node and the receiving of packets by the destination.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

*Number of loops formed:* The adversaries are capable of causing routing loops that prevent a node from discovering its neighbor.
*Packet dropping probability:* It is the probability of attackers to drop the packets.
*Location Error Rate:* It is defined as the fraction of distance deviated from the actual radio range per data flow.

### 6.3 Performance Evaluation

This section analyses the network performance in the presence of 40% attackers. It considers the effect of the most common attacks on geographic routing with the above discussed metrics.

#### 6.3.1 Impact on the Packet Delivery Ratio

The impact of position faking attack on the packet delivery ratio has been simulated with various percentages of position faking adversaries. Figure 7 shows the adversaries impact on the packet delivery ratio in which the 1000x1000 m sized network is simulated with 40% of location faking adversaries. The percentage of packet delivery ratio decreases with various location based attacks including position faking attacks, distance and time based attacks, and hyperbola based attack. The position faking attacks except greedy spoofing reduce the packet delivery ratio tremendously compared to the other attacks as they depends mainly on the position information. In position faking attack, the attacker claims the fake position that is unreachable i.e. out of its communication range. Therefore, the source node sends the packet to the unreachable fake position that leads to the packet drop. The adversary node in the distance based attack in the perimeter mode varies the distance information that is slightly deviated from the original information. The adversary claims the false distance so as to obtain the traffic. By falsely claiming the distance, the adversaries deliver the packets with an increased hop count between the void node and the destination in the perimeter mode. Therefore, the distance and time based attacks maintains an acceptable PDR. In the hyperbola attack, the packet delivery ratio is comparatively high as the source node has chances to select the non optimal greedy node. This is because; the adversary node in hyperbola attack monitors the activities of only the actual greedy node.

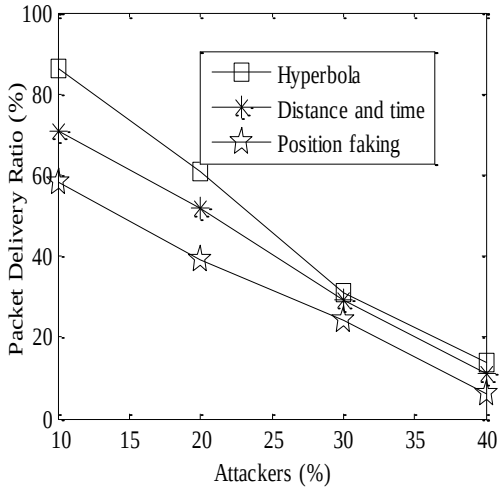

*Figure 7: Packet Delivery Ratio*

#### 6.3.2 Routing Overhead

The presence of location based adversaries considerably increases the routing overhead. Various behaviors of the location based adversary cause impacts on the overhead in various ranges. The distance and time based attack introduces a large overhead as it maintains the information of the time and distance between the void node to the destination. There is a need to maintain the information of reachable nodes that are involved in the perimeter mode but, the nodes involved in the perimeter mode are high compared to those in greedy mode. In hyperbola based attack, the adversary node claims the fake position on the hyperbola of the source and the greedy node and hence; the fake and original position information of the adversary is included in the source node‟s neighbor list. Whenever the packet forwarded to the fake position gets dropped, the source node re-transmits the packet. This process introduces additional overhead on the network. The position faking attacks cause a low overhead comparatively. The position faking attackers hide their own positions and claim only the fake positions and hence, introduce less overhead compared to distance and time, and the hyperbola attackers.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

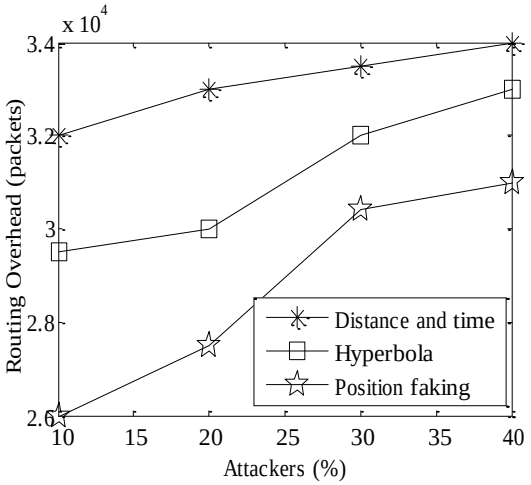


*Figure 8: Routing Overhead*

### 6.3.3 Average end-to-end delay

The average end-to-end delay caused by various location based attackers is shown in figure 9. The delay caused by the distance and time based attack is high compared to the position faking and hyperbola based attacks. The distance and time based attack is mainly launched in the perimeter mode whose main intention is to increase the hop length between the void nodes to the destination. It results in an extra delay in addition to the normal delay caused in the perimeter mode. The delay caused by the hyperbola based attack and position faking attack is almost the same. In these attacks, the source node is capable of determining the optimal path immediately after determining the packet drop caused by the adversary.

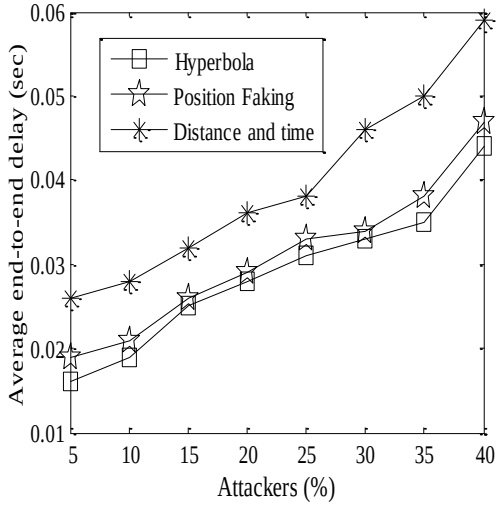


*Figure 9: Average end-to-end delay*

### 6.3.4 Impacts of Routing Loops

The number of routing loops formed by the distance and time based attack is high compared to the position faking and hyperbola based attacks. The distance and time based attacker exploits the right hand rule to launch the attack. In the perimeter mode, to avoid the packet traversing through the same link, it exploits the right hand rule for eliminating the crossing nodes. However, the distance and time based attack on perimeter routing varies the distance information to launch the attack. Hence, it forms the routing loop due to the distance variation. The hyperbola and position faking attacks form comparatively lesser number of loops. Some of the position faking attackers like tampering attackers fake their position with the main intention of loop formation. In hyperbola based attack, the possibility of routing loop formation is much low compared to the other attacks. The hyperbola based attackers just monitors the timing information and claim their fake positions on the hyperbola of source and actual greedy node. Therefore, the same node cannot be selected as a forwarding node once again.

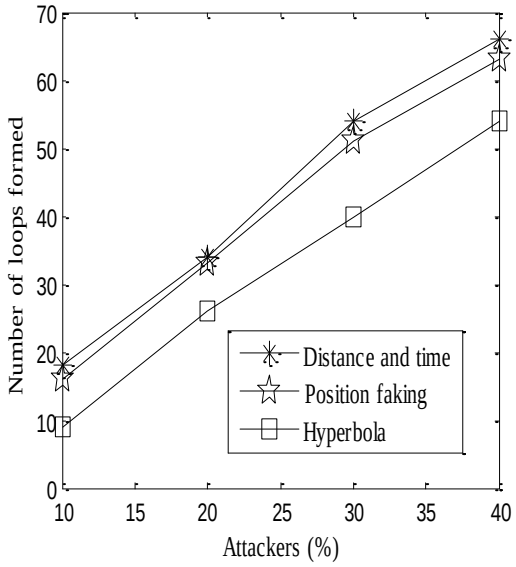


*Figure 10: Number of loops formed*

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

### 6.3.5 Packet Dropping Probability

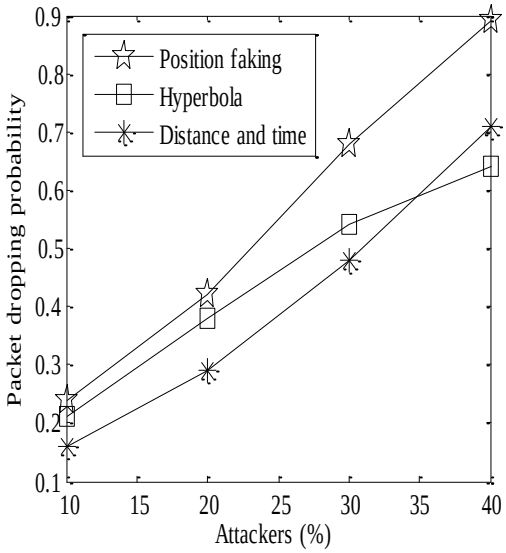


*Figure 11: Packet dropping probability*

The position faking attack has a high packet dropping probability as it claims its fake position mainly to drop the packets soon after acquiring the traffic. For instance, in the tampering attack, the attackers allow the packet to traverse on the loop formed and drop the packets after the TTL expires. In the greedy pretending attack, the attackers fake their position to drop the packets. Similarly, the hyperbola attacker claims the fake position such that a node resides on the hyperbola of the source and the greedy node. The source node transmits the packet to the claimed fake position that result in the packet drop. The packet dropping probability of the distance and time based attackers is comparatively low because its intention is to launch only the denial of service by increasing the hop count rather than dropping the packets. In the presence of 30-40 %attackers, the packet dropping probability of the distance and time based attack is suddenly increased. The packet gets dropped in the case of larger hop count as TTL of the packet expires before it reaches the destination.

### 6.3.6 Location Error Rate

The location error rate is high in the position faking attack. The position faking attackers claim the fake position that is unreachable. Therefore, there is much deviation from the original position of the attacker. In the hyperbola attack, the attacker claims a fake position that lies on the hyperbola of the source and the greedy node i.e. the attacker claims the fake position within its communication range. Therefore, the deviation from its original position is less, compared to position faking attack. In the distance and time based attack, an attacker deviates its position, such that it is closer than the any other optimal path in the perimeter mode.

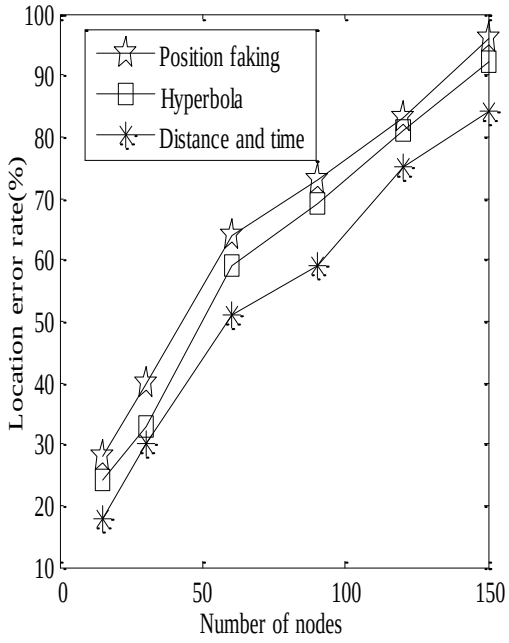


*Figure 12: Location Error Rate*

## 7. CONCLUSION

This work investigated the possible location based attacks in the geographic routing protocols. This work presented an analysis of effect of location based attacks on the network performance. It also listed out the other feasible attacks in geographic routing. The simulation has been conducted in the presence of 40% of each attacker and the results were analyzed. The simulation results prove that the overall routing performance decreases based on the behavior of the adversaries. Moreover, this work analyzed the major reason for decreased system performance. The major reasons for performance degradation by the adversaries are packet dropping and formation of routing loops. Finally, this work concludes that the location based attacks in MANET with geographic routing protocols results in severe routing performance degradation.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

**REFERENCES:**


[1] B. Karp and H. T. Kung, "GPSR: Greedy Perimeter Stateless Routing for Wireless Networks," in *Proceedings 6th ACM annual international conference on Mobile computing and networking*, 2000 (MobiCom '00), pp. 243–254.

[2] S. Basagni, I. Chlamtac, V. Syrotiuk, and B. Woodward, "A Distance Routing Effect Algorithm for Mobility (DREAM)" In *Proceedings of 4th Annual ACM/IEEE International Conference Mobile Computing and Networking*, 1998 pp. 76- 84.

[3] Y.-B. Ko and N. Vaidya "Location-aided routing (LAR) in mobile ad hoc networks" In Proc. 4th *ACM/IEEE International Conference on Mobile Computing and Networking,1998* pp. 66- 75.

[4] S. Gajurel, B. Malakooti, L. Want, "Re-Configurable Antenna & Transmission Power for Location Aware MANET Routing with Multiple Objective Optimization", *Journal of Networks (JNW)*, 2008 pp. 1796-2056, Vol.3, No. 3.

[5] W.-H. Liao, Y. C. Tseng, and J.P. Sheu "GRID: A fully location-aware routing protocol for mobile ad hoc networks" Springer, *Journal on Telecommunication Systems, 2001* Vol. 18, No- 1- 3, pp. 37 -60.

[6] P. Bose, P. Morin, I. Stojmenovic, and J. Urrutia, "Routing with guaranteed delivery in ad hoc wireless networks," in *Proceedings of 3rd international workshop on Discrete algorithms and methods for mobile computing and communications*, (DIALM '99), ACM, pp. 48–55.

[7] Mauve, M., Widmer, J, Hartenstein, H, "A survey on position-based routing in mobile ad-hoc networks", *IEEE transaction on Network*, 2001 Vol. 15, No. 6, pp.30- 39.

[8] Fraser Cadger, Kevin Curran, Jose Santos, and Sandra Moffett "A Survey of Geographical Routing in Wireless Ad-Hoc Networks", *IEEE Communications Surveys & Tutorials*, 2013 Vol. 15, No. 2, pp. 621- 653.

[9] Dinesh Ramasamy and Upamanyu Madhow, "Geographic Routing in Large-Scale MANETs" *Technical report*, 2012

[10] Elliott D. Kaplan and Christopher J. Hegarty "Understanding GPS Principles and Applications"

[11] B.W. Parkinson and S.W. Gilbert, NAVSTAR: global positioning system – ten years later, *Proceedings of the IEEE*, 1983 Vol. 71, No. 10, pp. 1177–1186.

[12] G. Dommety and R. Jain, Potential networking applications of global positioning systems (GPS), *Technical report TR- 24*, The Ohio State University, 1996

[13] Kim. Y, Lee J.J, and Helmy A, "Impact of location inconsistencies on geographic routing in wireless networks" *Proceedings of the 6th ACM international workshop on Modeling analysis and simulation of wireless and mobile systems*, 2003 pp. 124–127.

[14] S. Kwon and N. Shroff, "Geographic routing in the presence of location errors," *Computer Networks*, 2006 Vol. 50, no. 15, pp. 2902– 2917.

[15] P. Papadimitratos, A. Jovanovic, "GNSS-based Positioning: Attacks and Countermeasures," *IEEE conference on Military Communication (MILCOM)*, 2008.

[16] Ke Liu, Nael Abu-Ghazaleh, and Kyoung - Don Kang, "Location verification and trust management for resilient geographic routing", *Elsevier, Joint Parallel Distributed Computing,2007* Vol. 67, pp. 215 – 228.

[17] Nilothpal Talukder, and Sheikh Iqbal Ahamed, "Preventing Multi-query Attack in Location based Services", *proceedings of the third ACM conference on wireless network security*, 2010 pp. 25- 36.

[18] Yingying Chen, Wade Trappe, Richard P. Martin, "Attack Detection in Wireless Localization", *26th IEEE International conference on computer communications, INFOCOM*, 2007pp. 1964- 1972.

[19] Marco Fiore, Claudio Casetti, Carla-Fabiana Chiasserini, and Panagiotis Papadimitratos "Discovery and Verification of Neighbor Positions in Mobile Ad Hoc Networks", *IEEE transaction on mobile computing, 2011*

[20] Joo -Han Song, Vincent W.S. Wong, Victor C.M. Leung "Secure position-based routing protocol for mobile ad hoc networks" *Elsevier transaction on Ad Hoc Networks*,2007 Vol 5 pp. 76–86.