International Journal of Computer Information Systems and Industrial Management Applications
ISSN 2150-7988 Volume 3 (2011) pp. 271-279

A Study on Wormhole Attacks in MANET

Reshmi Maulik[1] and Nabendu Chaki[2]

[1] Meghnad Saha Institute of Technology, Techno Complex,
Madurdaha, Kolkata 700150, India
reshmimaulik@gmail.com

[2] Department of Computer Science and Engineering, University of Calcutta,
92 A. P. C. Road, Kolkata 700009, India
nabendu@ieee.org

***Abstract*: An Ad-hoc network is a self-organized network, without a central coordinator, and which frequently changes its topology. In this paper, we have analyzed the performance of Mobile Ad-hoc Networks (MANET) under wormhole attack. Multiple QoS parameters have been considered here such as throughput, delay, packet delivery ratio, node energy and node density. The NS2 network simulator has been used and the reference point group mobility model (RPGM) is considered to study the effect of node density and the initial energy on the throughput.**

***Keywords*:** MANET, intrusion detection, wormhole, packet delivery ratio, RPGM model**.**

I. Introduction

Mobile Ad-hoc Network (MANET) is formed by some wireless nodes communicating each other without having any central coordinator to control their function. Such a network is helpful in creating communication between nodes that may not be in line-of-sight and outside wireless transmission range of each other. Similar wireless networks have important applications in a wide range of areas covering from health [1], environmental control [2] to military systems. In MANET, as the nodes are utilizing open air medium to communicate, they face acute security problems compared to the wired medium. One such critical problem is wormhole attack. Under this attack, two faraway malicious nodes can collude together using either wired link or directional antenna, to give an impression that they are only one hop away. Wormhole attack can be launched in hidden or in participation mode. Wormholes can either be used to analyze the traffic through the network or to drop packets selectively or completely to affect the flow of information. The security mechanisms used for wired network such as authentication and encryption are futile under hidden mode wormhole attack, as the nodes only forward the packets and do not modify their headers. Attack in participating mode is more difficult, yet once it is launched, it is also hard to detect.

MANET faces several challenges. They include:

1) Multicast Routing – Designing of multicast routing protocol for a constantly changing MANET environment.

2) Quality of service (QoS) – Providing constant QoS for different multimedia services in frequently changing environment.

3) Internetworking – Communication between wired network and MANET while maintaining harmony.

4) Power Consumption – The necessity of conservation of power and discovery of power saving routing protocol.

In this article, we give a brief overview of the routing protocols used in MANET, as well a brief discussion on wormholes, their detection and avoidance. However, the most significant contribution of this article is a quantitative study of performance of different protocols under wormhole attack using NS2 network simulator. Similar performance analysis for packet loss replacement in VoIP by simulation using NS2 has been done in [3]. Some authors [1], [4] have used Opnet to do the simulation for performance analysis.

II. Routing Protocols and Wormhole Attack

Many routing protocols are available for MANET. In this section, some of the frequently used routing protocols are reviewed and the threat of wormhole attacks to such protocols is considered. These routing protocols can be categorized into two types: table-driven/proactive and demand-driven/reactive [5]. DSDV, OLSR and SEAD are proactive routing protocols; while DSR, AODV and Ariadne are reactive routing protocols.

A. DSDV (Destination Sequenced Distance Vector)

DSDV is a proactive routing protocol, where all the possible destination routes, the metric and next hop to each destination and sequence number generated by the destination node are maintained in a table [5], [6]. Each node acts as a router. The table is updated by periodic exchange of messages between neighboring routers. This protocol is vulnerable to wormhole attack [7]. The colluding nodes pass on message between two faraway nodes, say X and Y, using a tunnel. This will cause X and Y to view themselves as neighbors and they will, in turn, advertise a hop count of one between each other. Due to this false information, other authenticated nodes will try to send all the messages with destination Y through X, if the alternative route has hop count more than one. However, as they are outside the transmission range, they will fail to communicate.

B. OLSR (Optimized Link State Routing)

OLSR is a proactive routing protocol. Topology information is exchanged periodically. Hello messages are broadcast to discover single hop neighbors. To distribute signaling traffic, flooding mechanism is used where every node forwards a flooded message not forwarded by it earlier. Topology messages containing the information about link states are then sent to all other nodes. From this information, each node computes the shortest path using symmetric links to form a partial topology graph. It is open to wormhole attack [7] – [9]. Remote nodes may send hello and topology control messages available at its colluding nodes to its own neighbors for dissemination as false information into the network. This will make two faraway nodes to wrongly consider themselves as neighbors, leading to failure of routing protocol.

C. SEAD (Secure Ad-hoc Distance Vector)

The SEAD protocol is based on one-way hash chains rather than asymmetric cryptograph and prevents the network from uncoordinated attacks and DoS attacks. Some of the nodes have the capacity to authenticate all other elements of the chain. This requires authenticating the sequence number and the metric of the routing table. The receiver must also authenticate the sender [6]. Thus, an attacker, without compromising a node, cannot send routing message, as it cannot provide authentication code to its neighbors [10]. Though SEAD successfully handles replay attack, it is unable to cope up with wormhole attack [11] by a malicious node acting as a repeater and replaying the message from an unauthenticated node.

D. DSR (Dynamic Source Routing)

DSR is a reactive routing protocol as it discovers the address routes only when it has packets to send to that destination. It requires source route maintenance, since, during the use of the route, it is required to monitor the operation of the route and to inform the sender of any errors [6]. It is vulnerable to wormhole attack and may also result in denial of service attack at the destination [7]. This protocol requires forwarding of only the first RREQ received by it and will discard all other RREQ packets for the same route. The RREQ packet contains the information regarding the intermediate nodes and the hop count. The route discovered is then utilized to send data packets. As wormhole attack uses a fast channel for forwarding messages, the RREQ packet through them will reach destination faster compared to other paths. This will result in only the wormhole path to be discovered as the route to destination. The data packets may be fully or selectively discarded by the wormhole attacker resulting in permanent denial of service attack at the destination.

E. Aridane (A Secure On-Demand Routing Protocol for Ad-hoc Networks)

The Ariadne protocol is based on DSR and it depends on symmetric cryptography. Ariadne guarantees that the destination node authenticates the source and the source can authenticate each intermediate node in the route. Each intermediate node can remove or add nodes in the list of nodes of the route request. It uses the key administration protocol called TESLA which depends on the clock synchronization to authenticate routing messages. It uses per-hop hashing mechanism [6]. The authentication at each node not only depends upon the content of the RREQ packet but also the authentication code of the previous node. Ariadne is free from flooding of RREQ attack as the network-wide shared secret key prevents the attacker from replaying the message. Each node is required to add authentication code to each RREQ packet it forwards. The source node can verify the origin of each individual data field in the RREP message [12]. It is immune to wormhole attack and rushing attack as well [11] since successful route falsification requires RREQ to be modified carefully.

F. AODV (Ad-hoc On-demand Distance Vector)

It is a pure on-demand routing protocol. For sending messages to destination, it broadcasts RREQ messages to its immediate neighbors. These neighbors in turn rebroadcast them to their neighbors. This process continues unless the RREQ message reaches the destination. Upon receiving the first RREQ message from the source node, it sends a RREP to the source node following the same reverse path [5], [13]. All the intermediate nodes also set up forward route entries in their table. Upon detecting error in any link to a node, the neighboring nodes forward route error message to all its neighbors using the link. These again initiate a route discovery process to replace the broken link. The AODV routing protocol is vulnerable to wormhole attack [7]. Since the colluding nodes involved in wormhole attack uses a high speed channel to send messages, it is possible that the RREQ packet through them reaches the destination faster compared to usual path. According to this protocol, the destination discards all the later RREQ packets received, even though they are from authenticated node. The destination therefore chooses the false path through wormhole for RREP [5].

III. Wormholes and Its Variants

This paper focuses on the wormhole attack, where two colluding nodes that are far apart are connected by a tunnel giving an illusion that they are neighbors. Each of these nodes receive route request and topology control messages from the network and send it to the other colluding node via tunnel which will then replay it into the network from there. By using this additional tunnel, these nodes are able to advertise that they have the shortest path through them. Once this link is established, the attackers may choose each other as multipoint relays (MPRs), which then lead to an exchange of some topology control (TC) messages and data packets through the wormhole tunnel. Since these MPRs forward flawed topology information, it results in spreading of incorrect topology information throughout the network [8]. On receiving this false information, other nodes may send their messages through them for fast delivery. Thus, it prevents honest intermediate nodes from establishing links between the source and the destination [11]. Sometimes, due to this, even a wormhole attacker may fall victim to its own success.

In [9], a particular type of wormhole attack known as “in-band wormhole attack” is identified. A game theoretic approach has been followed to detect intrusion in the network. Presence of a central authority is assumed for monitoring the network. This is a limitation in wireless scenario such as military or emergency rescue. No experimental result is reported in [9].

In [14] the wormhole attacks are classified as 1) In-band

wormhole attack, which require a covert overlay over the existing wireless medium and 2) Out-of-band wormhole attack, which require a hardware channel to connect two colluding nodes. The in-band wormhole attacks are further divided in [14] as 1.1) Self-sufficient wormhole attack, where the attack is limited to the colluding nodes and 1.2) Extended wormhole attack, where the attack is extended beyond the colluding nodes. The colluding nodes attack some of its neighboring nodes and attract all the traffic received by its neighbor to pass through them.

In the second type of wormhole attacks [15], the intrusions are distinguished between a) hidden attack, where the network is unaware of the presence of malicious nodes and b) exposed attack, where the network is aware of the presence of nodes but cannot identify malicious nodes among them.

IV. Prevention of Wormhole Attack

Choi et al. in [16] considered that all the nodes will monitor the behavior of its neighbors. Each node will send RREQ messages to destination by using its neighbor list. If the source does not receive back the RREP message within a stipulated time, it detects the presence of wormhole and adds the route to its wormhole list. Each node maintains a neighbor node table which contains a RREQ sequence number, neighbor node ID, sending time and receiving time of the RREQ and count. Here the source node sets the Wormhole Prevention Timer (WPT) after sending RREQ packet and wait until it overhears its neighbor's retransmission. According to the author, the maximum amount of time required for a packet to travel one-hop distance is WPT/2. Therefore, the delay per hop value must not exceed estimated WPT. However, the proposed method does not fully support DSR as it is based on end-to-end signature authentication of routing packets.

Mahajan et al. [14] proposed some proposals to detect wormhole attacks like:

1) The abrupt decrease in the path lengths can be used as a possible symptom of the wormhole attack.

2) With the available advertised path information, if the end-to-end path delay for a path cannot be explained by the sum of hop delays of the hops present on its advertised path, existence of wormhole can be suspected.

3) Some of the paths may not follow the advertised false link, yet they may use some nodes involved in the wormhole attack. This will lead to an increase in hop delay due to wormhole traffic and subsequently an increase in end-to-end delay on the path. An abrupt increase in the end-to-end delay and the hop queuing delay values that cannot be explained by the traffic supposedly flowing through these nodes can lead us to suspect the presence of wormhole.

V. Detection and Avoidance of Wormhole Attacks

Detection of wormhole has been an active area of research for past few years. The major task is to find out the presence of wormhole in the network [8], [17] – [24].

In [19], detection of wormhole nodes is done on the basis of the Hello control messages. As a metric of compliance with the OLSR specifications, the author has used the percentage of HELLO Message Timing Intervals (HMTIs) that lie within a range bounded by the amount of jitter. A range $R = [T - \delta, T + \delta]$ has been defined. If an HMTI is in this range R, it is considered to be valid; otherwise it is out-of-protocol. A secondary check is done whenever the Hello Message Timing Interval packet behavior is suspicious. On the other hand, a poorly performing node would have associated with it a relatively large number of retry packets, which would not be the case with an attacking node. This way, the problem of false positive alarms is negotiated.

In [17], a new protocol called Multi-path Hop-count Analysis (MHA) is introduced based on hop-count analysis to avoid wormhole attack. It is assumed that too low or too high hop-count is not healthy for the network. The novelty of the hop-count analysis in detecting wormholes is however questionable. Similar works have also been reported earlier. As an example, Djenouri et al. [18] may be considered.

In [8], wormholes are detected by considering the fact that wormhole attacks consists of relatively longer packet latency than the normal wireless propagation latency on a single hop. Since the route through wormhole seems to be shorter, many other multi-hop routes are also channeled to the wormhole leading to longer queuing delays in wormhole. The links with delays are considered to be suspicious links, since the delay may also occur due to congestion and intra-nodal processing. The OLSR protocol has been followed as the basis for routing. The approach [8] aims to detect the suspicious link and verify them in a two step process described below.

In the first step, Hello packets are sent to all the nodes within its transmission range. When the receiver receives a Hello (request), it records the sender's address and the time delay Δ left until it is scheduled to send its next Hello message. For piggybacked reply, the node attaches the recorded address of the sender and their respective values of Δ. When a node receives a Hello (reply), it checks whether it contains information related to any of its outstanding requests. If no such information is present, then it treats it as any other control packet. Otherwise, the node checks the arrival time of Hello (reply) to see whether it arrived within its scheduled timeout interval taking into consideration the delay Δ that occurred at the receivers end. If it is within its timeout then the link between itself and node is considered to be safe, otherwise suspicious and communication to that node is suspended by the sender nodes until the verification procedure is over.

In the second step, the sender will send a probing packet to all the suspected nodes detected in the previous step.

If a proper acknowledgement is received from some node X within its scheduled timeout then node X is again considered to be safe. Otherwise the presence of wormhole is proved. Further the end-to-end authentication is also considered by using symmetric key cryptography.

In reference [15], both the hop count and delay per hop indication (DelPHI) are monitored for wormhole detection. The fundamental assumption in [15] is once again that the delay a packet experiences under normal circumstances for propagating one hop will become very high under wormhole attack as the actual path between the nodes is longer than the advertised path. Like [8], the proposed methodology in [15] for wormhole detection is also a two-step process.

In the first phase the route path information are collected from a set of disjoint paths from sender to receiver. Each sender will include a timestamp on a special DREQ packet and sign it before sending it to the receiver. Each node upon receiving the packet for first time will include its node ID and increase the hop count by 1 and discards the packet next time

onwards. The DREP packets will be sent by the receiver for each disjoint path received by it. This procedure is carried out for three times and the shortest delay as well as hop count information will be selected for wormhole detection. In the second phase, the round trip time (RTT) is taken by calculating the time difference between the packet it had sent to its neighbor and the reply received by it. The delay per hop value (DPH) is calculated as RTT/2h, where h is the hop count to the particular neighbor. Under normal circumstances, a smaller h will also have smaller RTT. However, under wormhole attack, even a smaller hop count would have a larger RTT. If one DPH value for node X exceeds the successive one by some threshold, then the path through node X to all other paths with DPH values larger than it is treated as under wormhole attack.

$Pi = ni / N$, for all Ii

$Pmax = max\ (Pi)$,

where R is the set of all obtained routes, Ii is the ith link, ni is the number of times that Ii appears in R, N is the total number of links in R, and Pi is the relative frequency that Ii appears in R. If $Pmax > Pthreshold$, check the trust information available in the RREP of that route. If the value of correlation coefficient for packets dropped to that sent is greater than the pre-set threshold t, then the node is malicious, inform the operator else continue with routing process.

Both in [22], [23], it has been established that the normal link frequency analysis may lead to false detection of wormhole attacks. However, these identify the behavior of a wormhole as they keep track of the total number of packet drops rather than the pattern of drop.

Table 1. Summary of detection methods of wormhole attack.

Method	Mobility	QoS Parameter	Synchronization	False detection
HMTIs [19]	Handled weakly. Topologically robust, short range worm-hole can be detected.	Jitter and delay.	Not required. Since PSD profiling is done locally.	Used PSD to detect false positive alarm.
Farid et al. [8]	Not considered.	Packet processing time, queue delays within nodes.	Some time delay added to detect suspicious links.	Not handled.
DelPHI [15]	Not considered.	Delay.	Not required.	Not handled.
SAM [20]	Cluster and uniform topology considered.	Not considered.	Not considered.	Not handled.
SaW [22]	Not considered	Not considered.	Not considered.	Failed to detect.
DaW [23]	Not considered.	Delay parameter.	Not considered.	Failed to detect.
WAP [16]	Maximum transmission distance is calculated.	Delay per hop.	Only the source node is synchronized.	Not handled.
WORMEROS [24]	Topological change is not considered.	Not considered.	Time synchronization not required. RTT between source node and destination node is considered.	Both false positive and false negative alarms are considered.

Both in SaW [22] and DaW [23], similar propositions are made. Only difference is in the selection of routing protocols. In reference [22], AODV protocol was followed while in [23], DSR routing protocol was used. In both of these papers, trust based security models have been proposed and used to detect intrusion. Statistical methods have been used to detect the attacks. If any link is found to be suspicious, then available trust information is used to detect whether the link is a wormhole. In the trust model used, nodes monitor neighbors based on their packet drop pattern and not on the measure of number of drops. Karl Pearson's formula for correlation coefficient is used in identifying the pattern of the drops. In [23], another algorithm for detecting the presence of wormhole in the network has been proposed. Here, after sending the RREQ, the source waits for the RREP. The source receives many RREP coming through different routes. The link with very high frequency is checked using the following expression:

In [20], the wormhole attack is detected on multipath routing. When a source needs a new route, it will flood the network with RREQ and wait for responses. The intermediate node will forward the first RREQ packet only. The destination will wait for some time to collect all the obtained routes after receiving the first RREQ. A new scheme called Statistical Analysis of Multi-path (SAM) is proposed in [20]. SAM uses $Pmax$ and $\emptyset$, which will be higher in the presence of wormhole attack. Here, $Pmax$ is the maximum probability of relative frequency of a link to occur in the set of all obtained routes from one route discovery. $\emptyset$ is the difference between the most frequently appeared link and the second most frequently appeared links in the set of all obtained routes from one route discovery. A probability mass function (PMF) is used to find that the highest relative frequency is more for a system under wormhole attack as compared to a normal system. The

performance of on-demand multipath routing (MR) protocol and DSR are compared under wormhole attack.

In [21], WHIDS, a cluster based counter-measure is proposed for the wormhole attack. Simulation results using MATLAB exhibit the effectiveness of WHIDS for detecting wormhole attack. The method, however, has not been tested in presence of multiple wormhole attacks.

Vu et al. [24] also proposed to detect the presence of wormhole using two phases as in [8] and [15]. The first phase consists of two methods. In the first method, the measure of round-trip-time (RTT) between the source node and all of its immediate neighbors are considered. In the second method, source node identifies the one-hop and two-hop neighbors to form its neighbor set. If it is found that the destination node is not a neighbor of the source node then the link between them comes under suspicion. After detecting the suspicious links, the next phase is to confirm the existence of wormholes by using the RTS / CTS mechanism for exchange of messages.

Table 1 presents a multi-aspect qualitative comparison between eight different wormhole detection techniques discussed above. Important aspects like the node mobility, false alarm detection along QoS parameters have been considered for each detection approach. This qualitative analysis has been supported by a quantitative one as well for some of the algorithms using the network simulator tool. The results have been summarized in section 7.

VI. Metric to Detect Wormhole

There are different metrics to measure the strength of wormhole present in the network. Mahajan et al. [14] considered several metrics for measuring the capability of the nodes involved in wormhole attack. These include strength, length, attraction and robustness. These are defined below.

1) Strength: It is the amount of traffic attracted by the false link advertised by the colluding nodes.

2) Length: Larger the difference between the actual path and the advertised path, more anomalies can be observed in the network.

3) Attraction: This metric refers to the decrease in the path length offered by the wormhole. If the attraction is small then the small improvements in normal path may reduce its strength.

4) Robustness: The robustness of a wormhole refers to the ability of the wormhole to persist without significant decrease in the strength even in the presence of minor topology changes in the network.

Besides these, the packet delivery ratio which is the number of packet of delivered divided by the total number of packets dispatched forms a basic metric to quantify the impact of intrusion.

VII. Quantitative Study with Simulation

A. Simulation Environment

The NS2 (version 2.34) network simulator has been used for simulation work. The mobility scenarios are generated by a Random waypoint model and Reference Point Group Mobility Model (RPGM). The numbers of nodes tested in a terrain area of 600m x 800m are 50 and 100. The simulation parameters are summarized in Table 2. A new routing agent called wormhole AODV is added to include the wormhole attack. Here, 0 and 21 are posed as malicious nodes and the required coding is done so that they together form a wormhole link [25].

Table 2. Summary of Parameters Used for Simulation.

Parameter	Value
Terrain Area	600m X 800m
Simulation Time	300s
Number of nodes	50/ 100
Routing Protocol	AODV/ DSR
Traffic Model	CBR
Pause Time	1s
Initial Energy (in Joule)	1/ 2/10/15/20
Minimum Node Speed (m/s)	0
Maximum Node Speed (m/s)	2/3/5/10/15/20/30
Number of Sources	2/5/ 10/ 20/ 35/ 45
Transmission Power (mW)	0.6
Residual Power (mW)	0.3
Packet Size	512 Bytes
Mobility Model	Random Way Point/RPGM
Number of wormhole link	0, 1

Random Way Point mobility model is the most commonly used model for research purpose. Here all the nodes are randomly distributed with uniform speed. It includes pause time between changes in destination and speed. Pause time is used to overcome sudden stop and start in random way point model.

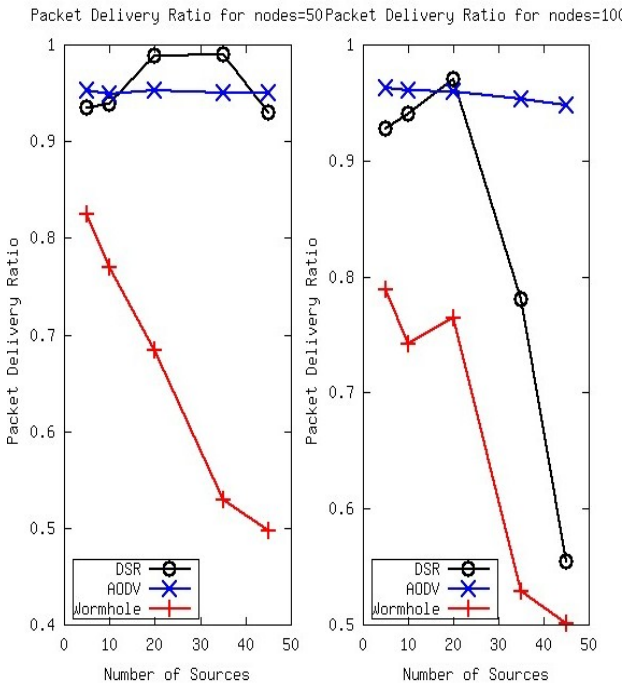

Figure 1: Packet Delivery ratio with wormhole link

B. Simulation Results and Analysis

Figure 1 describes the dependence of the packet delivery ratio on the number of sources in action. Two different scenarios have been considered corresponding to two different choices of total number of nodes being 50 and 100. The performance is similar in either case. The packet delivery ratio for AODV

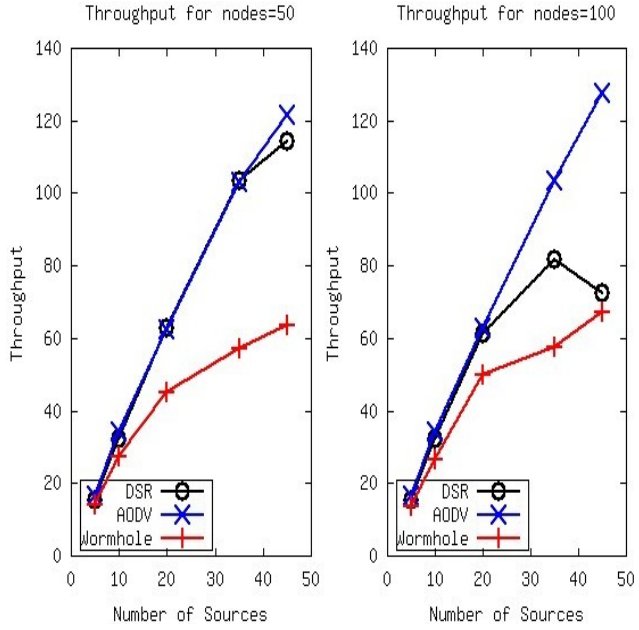

Figure 2: Throughput with wormhole link

remains invariant of the number of sources. For DSR, the packet delivery ratio produces a bell-shaped curve. It increases with the number of source initially and then shows a fall. The fall is steeper when the number of nodes is 100. At its highest, DSR performs better than AODV in either case. However, the performance in presence of wormhole declines drastically as expected and it shows a downward trend with the number of sources for both counts of nodes.

Figure 2 analyzes the same scenarios for throughput instead of the packet delivery ratio. In all three cases, namely, DSR, AODV and in the presence of wormhole, throughput increases with the number of sources. Again, AODV performs the best.

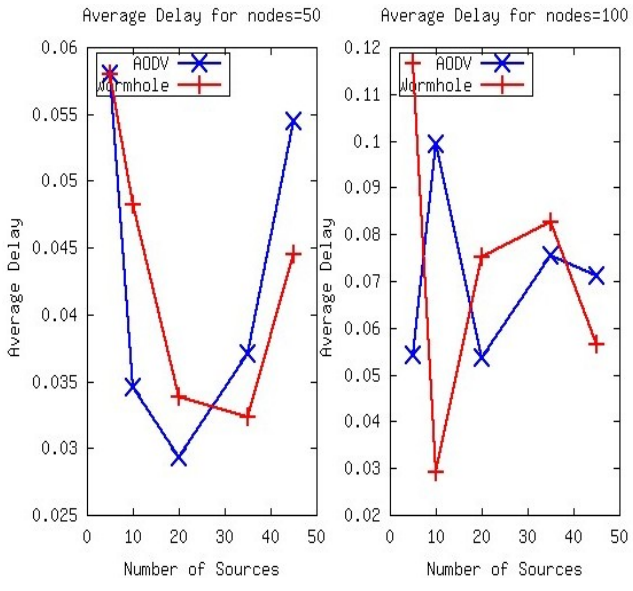

Figure 3: Delay in presence of wormhole link

DSR keeps up with the performance of AODV when the total number of nodes is 50. However, in the other case, throughput for DSR starts showing a drop as the number of sources increases. For a small number of sources, the presence of wormhole does not affect throughput much. However, the growth in throughput with the number of sources is much slower in presence of wormhole. This behavior can be explained by the congestion in the network as the time taken to reach destination may exceed the time-to-live counter mentioned in the header of the packet. On the other hand, as we increase the number of normal nodes, throughput also increases as the usage of the wormhole link for sending data packets falls.

Figure 3 considers the average delay in the same setup, but we consider only AODV and the presence of wormhole. No definite pattern emerges when the number of nodes is 100. Even the performance of AODV over the performance in presence of wormhole is not clearly illustrated. However, when the number of nodes is 50, the average delay produces an U-shaped curve. While AODV performs better initially, its performance becomes worse than that in the presence of wormhole as the number of source increases.

Next, we introduce RPGM to model the mobility issues. In the earlier analyses, we considered Random waypoint model only. RPGM model allows us to understand the effect of the node density. We allow the nodes to form clusters. A cluster of nodes communicates within the groups. Each group has a logical center (group leader) and all the group members are randomly distributed around the reference point. Every node has a speed and direction that is derived by randomly deviating from the group leader. The mobility of the group members is determined by the group leader. Such group mobility model is used during military and rescue operations.

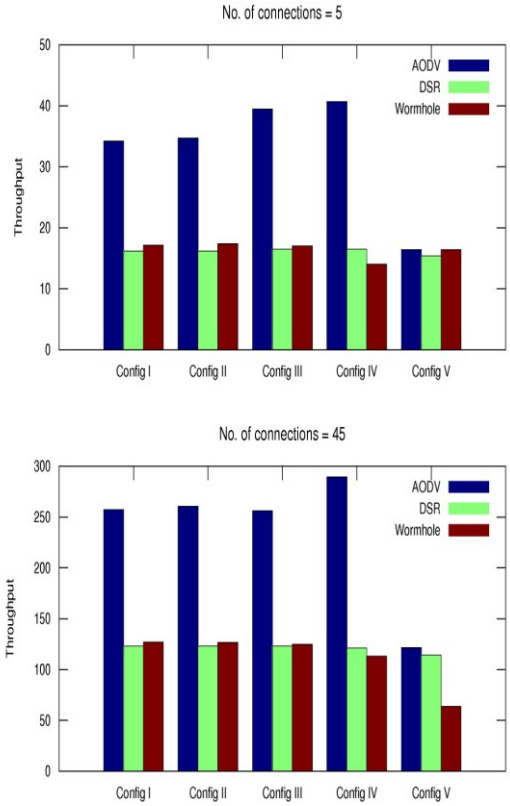

Figure 4: Throughput vs Node Density in presence of wormhole link

Five configurations with 50 nodes each have been configured:

Configuration I: 5 groups with 10 nodes each.

Configuration II: 3 groups consisting of 20, 20, 10 nodes.

Configuration III: 4 groups consisting of 5, 10, 15 and 20 nodes.

Configuration IV: 10 groups with 5 nodes each.

Configuration V: 50 nodes are dispersed using random way point mobility model.

It is clear from Figure 4 that throughput under RPGM model is greater than throughput under Random way point model for AODV. For a small number of connections, the throughput remains invariant in presence of wormhole, But for

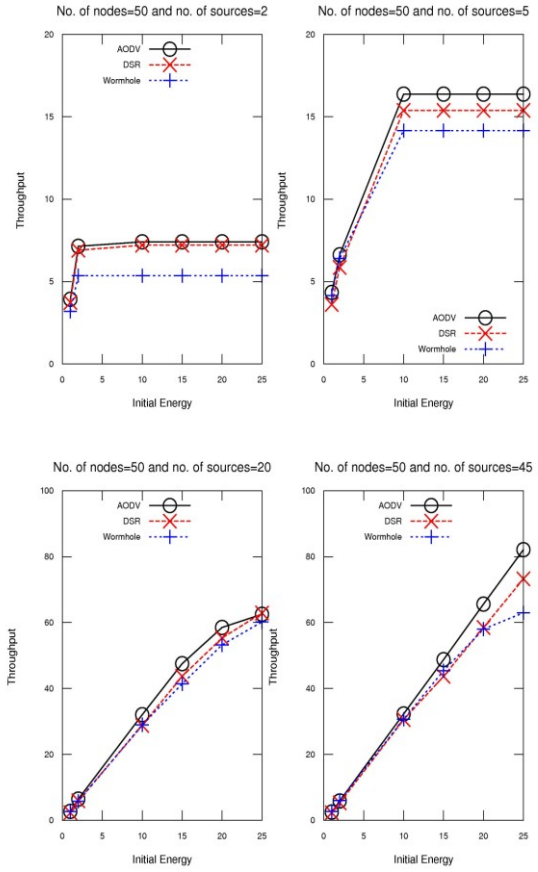

Figure 5: Throughput vs Node Energy in presence of wormhole link and random way point mobility

large number of connections, throughput drops under Random waypoint model in presence of wormhole. The performance remains invariant under DSR for either choice of number of connections. For all the setups, throughput increases with the number of connections. In the animation produced by the NS, it can be observed that throughput increases when the clusters of nodes are close to each other. However, when the clusters of nodes are too close to each other then the throughput may fall a little bit. The observation is in conformity with [26], [27].

Almost all ad-hoc mobile nodes depend upon the battery for their energy which is limited in practice. For every packet transmitted or received by the node, certain amount of power is consumed. Transmission requires more power compared to reception of packets. When the power falls to zero level, no further packets communication through the node is possible. We have made the following changes in the node configuration given in [28] to make the nodes energy aware.

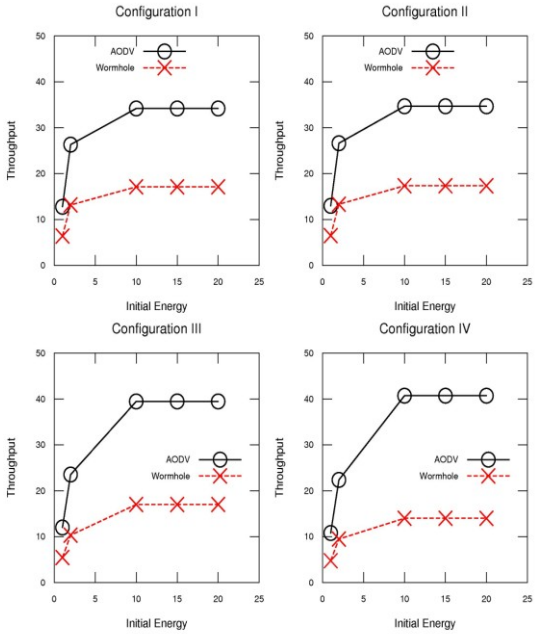

Figure 6: Throughput vs Energy in presence of wormhole link, node density and number of sources = 5

```
$ns_ node-config \
   -energyModel EnergyModel
   -initialEnergy 10.0
-txPower 0.6
-rxPower 0.3
```

Figure 5 shows the effect of the initial energy of the nodes on throughput level. There is a clear ordering in performance with AODV performing the best, followed by DSR and the performance in presence of wormhole being the worst. We have considered Random waypoint model here. The energy level is measured in Joules. The dependence of throughput on the initial energy level becomes more pronounced with the

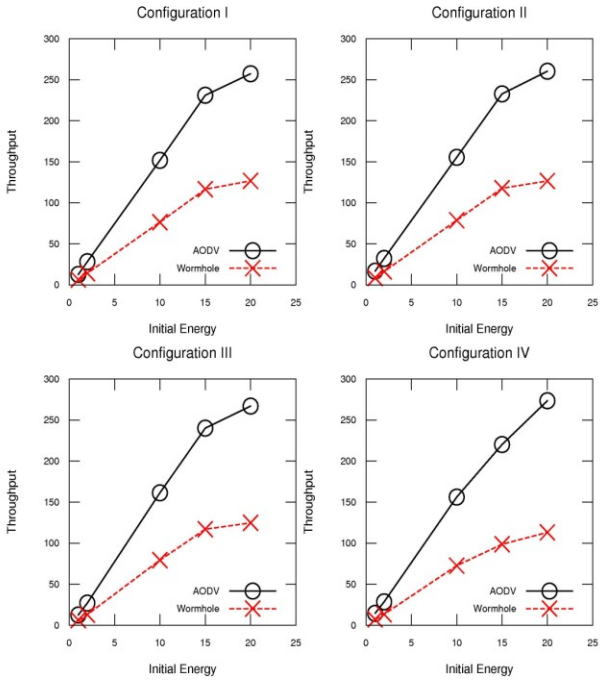

Figure 7: Throughput vs Energy in presence of wormhole link, node density and number of sources = 45

increase in the number of sources.

Figures 6 and 7 provide the same analysis under RPGM model. Number of sources is 5 in Figure 6, while it is taken as 45 in Figure 7. Since the performance of DSR is very similar to AODV, we illustrate AODV only together with the effect of the presence of wormhole.

As expected, throughput increases with number of sources involved. It is evident by comparing the scales of the graphs in Figures 6 and 7. As in the Random waypoint model, for RPGM model too, the effect of initial energy is low for smaller number of sources. The effect of initial energy ceases to exist beyond 10J, for both AODV and in presence of wormholes. The effect is more persistent with higher number of sources. However, throughput under wormhole attack falls drastically under the RPGM model compared to the Random waypoint model.

VIII. Conclusion

In this paper, an exhaustive simulation for MANET is done using AODV and DSR routing protocols and the effect of the presence of wormhole is also simulated. Significant QoS parameters such as throughput, delay, node density, packet delivery ratio and power consumption have been considered. The study focuses on how QoS is affected under wormhole attack in a network. The study here establishes the foundation for future work towards designing a mechanism to identify the nodes and the links which are actively involved in the wormhole attack.

References

[1] Norman A. Benjamin, Suresh Sankaranarayan. "Performance of Wireless Body Sensor based Mesh Network for Health Application", *International Journal of Computer Information Systems and Industrial Management Applications,* 2, pp. 20-28, 2010.

[2] Masayuki Nakamura, Atsushi Sakurai, Jiro Nakamura. "Autonomic Wireless Sensor/Actuator Networks for Tracking Environment Control Behaviors", *International Journal of Computer Information Systems and Industrial Management Applications,* 1, pp. 125-132, 2009.

[3] K. Maheswari, M. Punithavalli. "Performance Evaluation of Packet Loss Replacement using Repetititon Technique in VoIP Streams", *International Journal of Computer Information Systems and Industrial Management Applications,* 2, pp. 289-296, 2010.

[4] M. Rajput, P. Khatri, A. Shastri, K. Solanki. "Comparison of Ad-hoc Reactive Routing Protocols using OPNET Modeler". In *Proceedings of International Conference on Computer Information Systems and Industrial Management Applications,* pp. 7-12, 2010.

[5] R.H. Khokhar, Md. A.Ngadi, S. Manda. "A Review of Current Routing Attacks in Mobile Ad Hoc Networks", *International Journal of Computer Science and Security*, 2 (3), pp. 18-29, 2008.

[6] D. Vivian, E.A.P. Alchieri, C.B. Westphall. "Evaluation of QoS Metrics in Ad Hoc Networks with the use of Secure Routing Protocols". In *Network Operations and Management Symposium*, pp. 1-14, 2006.

[7] Yih-Chun Hu, Adrian Perrig, David B. Johnson. "Packet leashes: A Defense against Wormhole Attacks in Wireless Ad Hoc Networks". In *22nd Annual Joint Conference of the IEEE Computer and Communications Societies(INFOCOM) ,* 3, pp. 1976-1986, 2003.

[8] F. Nait-Abdesselam, B. Bensaou, T. Taleb. "Detecting and Avoiding Wormhole Attacks in Wireless Ad hoc Networks", *IEEE Communications Magazine*, 46 (4), pp. 127 - 133, 2008.

[9] John S. Baras, Svetlana Radosavac, George Theodorakopoulos. "Intrusion Detection System Resiliency to Byzantine Attacks: The Case Study of Wormholes in OLSR". In *IEEE Military Communications Conference (MILCOM)*, pp. 1-7, 2007.

[10] Y.-C. Hu, A. Perrig, D.B. Johnson. "SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks". In *Proceedings of Fourth IEEE Workshop on Mobile Computing Systems and Applications*, pp. 3- 13, 2002.

[11] Kamanshis Biswas, Md. Liakat Ali. "Security Threats in Mobile Ad Hoc Network". Thesis Paper submitted to the Department of Interaction and System Design, School of Engineering at Blekinge Institute of Technology, Thesis no: MCS-2007:07, 2007.

[12] Y.-C. Hu, A. Perrig, D.B. Johnson. "Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks", *Wireless Networks*, 11(1-2), pp. 21–38, 2005.

[13] Bounpadith Kannhavong, Hidehisa Nakayama, Yoshiaki Nemoto, Nei Kato, Abbas Jamalipour. "A Survey of Routing Attacks in Mobile Ad Hoc Networks", *IEEE Wireless Communication*, 14 (5), pp. 85-91, 2007.

[14] V. Mahajan, M. Natu, A. Sethi. "Analysis of wormhole intrusion attacks in MANETS". In *IEEE Military Communications Conference (MILCOM)*, pp. 1-7, 2008.

[15] H.S. Chiu and K. Lui. "DelPHI: Wormhole Detection Mechanism for Ad Hoc Wireless Networks". In *Proceedings of International Symposium on Wireless Pervasive Computing,* pp. 6-11, 2006.

[16] S. Choi, D. Kim, D. Lee, J. Jung. "WAP: Wormhole Attack Prevention Algorithm in Mobile Ad Hoc Networks". In *International Conference on Sensor Networks, Ubiquitous and Trustworthy Computing*, pp. 343-348, 2008.

[17] Shang-Ming Jen, Chi-Sung Laih, Wen-Chung Kuo. "A Hop-Count Analysis Scheme for Avoiding Wormhole Attacks in MANET", 9 (6), pp. 5022-5039, 2009.

[18] D. Djenouri, O. Mahmoudi, D. Llewellyn-Jones, M. Merabti, "On Securing MANET Routing Protocol Against Control Packet Dropping". In *IEEE International Conference on Pervasive Services*, pp. 100-108, 2007.

[19] M.A. Gorlatova, P.C. Mason, M. Wang, L. Lamont, R. Liscano, "Detecting Wormhole Attacks in Mobile Ad Hoc Networks through Protocol Breaking and Packet Timing Analysis". In *IEEE Military Communications Conference*, pp. 1-7, 2006.

[20] N. Song, L. Qian, X. Li. "Wormhole Attacks Detection in Wireless Ad Hoc Networks: A Statistical Analysis Approach". In Proceedings of the 19th IEEE *International Parallel and Distributed Processing Symposium*, pp. 8-15, 2005.

[21] D.B. Roy, R. Chaki, N. Chaki. "A New Cluster-based Wormhole Intrusion Detection Algorithm for Mobile Ad-hoc Networks", *IJNSA*, 1 (1), pp. 44-52, 2009.

[22] M.S. Sankaran, S. Poddar, P.S. Das, S. Selvakumar. "A Novel Security model SaW: Security against Wormhole attack in Wireless Sensor Networks". In *Proceedings of International Conference on PDCN*, 2009.

[23] Khin Sandar Win. "Analysis of Detecting Wormhole Attack in Wireless Networks", *World Academy of Science, Engineering and Technology*, 48, pp. 422-428, 2008.

[24] H. Vu, A. Kulkarni, K. Sarac, N. Mittal. "WORMEROS: A New Framework for Defending against Wormhole Attacks on Wireless Ad Hoc Networks". In *Proceedings of International Confernce on Wireless Algorithms Systems and Applications*, LNCS 5258, pp. 491-502, 2008.

[25] R. Maulik, N. Chaki. "A Comprehensive Review on Wormhole Attacks in MANET". In *Proceedings of 9th International Conference on Computer Information Systems and Industrial Management Applications*, pp. 233-238, 2010.

[26] Geetha Jayakumar, Gopinath Ganapathi. "Reference Point Group Mobility and Random Waypoint Models in Performance Evaluation of MANET Routing Protocols", *Journal of Computer Systems, Networks, and Communications*, 2008.

[27] Lee K. Thong. "Performance Analysis of Mobile Adhoc Network Routing Protocols". Thesis Paper submitted to the Department of Computer Science, Naval Post Graduate School, Monterey, CA, 2004.

[28] NS-2 Documentation. http://www.isi.edu/nsnam/ns/.

Author Biographies

Reshmi Maulik is an Assistant Professor in Meghnad Institute of Technology, Techno India Group, Kolkata, India. She received her Master's degree in Economics from University of Calcutta in 2000. She then completed C level (equivalent to M.Tech. in Computer Science) from DOEACC Society, Government of India, in 2005. She has also worked in the software industry for 3 years before returning to academia. Her current research focuses on mobile adhoc network (MANET), performance analysis of protocols and network security.

Nabendu Chaki is a faculty member in the Department of Computer Science & Engineering, University of Calcutta, Kolkata, India. He did his first graduation in Physics and then in Computer Science & Engineering, both from the University of Calcutta. He has completed Ph.D. in 2000 from Jadavpur University, India. Dr. Chaki has authored a couple of text books and more than 70 refereed research papers in Journals and International conferences. His areas of research interests include distributed computing, bio-informatics and software engineering. Dr. Chaki has also served as a Research Assistant Professor in the Ph.D. program in Software Engineering in U.S. Naval Postgraduate School, Monterey, CA. He is a visiting faculty member for many universities including the University of Ca'Foscari, Venice, Italy. Dr. Chaki is a Knowledge Area Editor in Mathematical Foundation for the SWEBOK project of the IEEE Computer Society. Besides being in the editorial board for four International Journals, he has also served in the committees of more than 40 international conferences.