International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

Security Schemes to Resolve Wormhole Attack in Distributed Sensor Networks

Sharada Y. Yalavigi[1], Dr. Krishnamurthy G. N[2], Dr. Nandini Sidnal[3]

Abstract: ***Distributed Sensor Networks (DSN) is an emerging technology and has a wide range of applications such as Environment (habitat) monitoring, Seismic monitoring, Terrain Surveillance, etc. The security of a sensor network is a critical aspect because of the random deployment of sensor nodes in an unattended environment. Distributed sensor networks are vulnerable against various types of external andinternal attacks being limited by computation resources, smaller memory capacity, limited battery life,processing power & lack of tamper resistant packaging.The network's broadcasting character and transmissionmedium help the attacker to interrupt network. An attacker can transform the routing protocol andinterrupt the network operations through mechanisms such as selective forwarding, packet drops,and data fabrication. One of the serious routing-disruption attacks is Wormhole Attack. The mainemphasis of this paper is to study wormhole attack, its detection method and the different techniquesto prevent the network from this attack.***

Keywords: Hello flood attack, Denial of service attacks, wormhole attack, Distributed, Sensor Networks

1. Introduction

Sensor Networks can be viewed as a distributed autonomous system for information gathering, performing data-intensive tasks such as environment (habitat) monitoring, seismic monitoring, battlefield surveillance, etc. The elements of the sensor networks are Sink, which sends queries and collects data from sensors and sensor which monitors phenomenon and reports to sink through wireless links. These wireless links are more prone to attacks than the wired networks. The coverage, connectivity and energy related issues are very important in Distributed Sensor Networks (DSNs). The most critical aspect of sensor network is "SECURITY". In applications like defense (military) without security the use of Sensor Network in any application would result in disastrous consequences. Security allows Sensor Networks to be used to maintain integrity of data and availability of all messages in the presence of resourceful adversaries. The main objective of confidentiality and authenticity is expected in sensor networks to safe guard the information traveling among the nodes of the network or between the sensor nodes and the sink node from disclosure. The DSNs are comprised of a group of nodes for scalar or multidimensional data gathering. Sensor nodes are employed to collect the information, compress and process it for storage purpose and to transmit the processed data to a sink. The transmitted information is then presented to the system by this sink connection as shown in figure1.

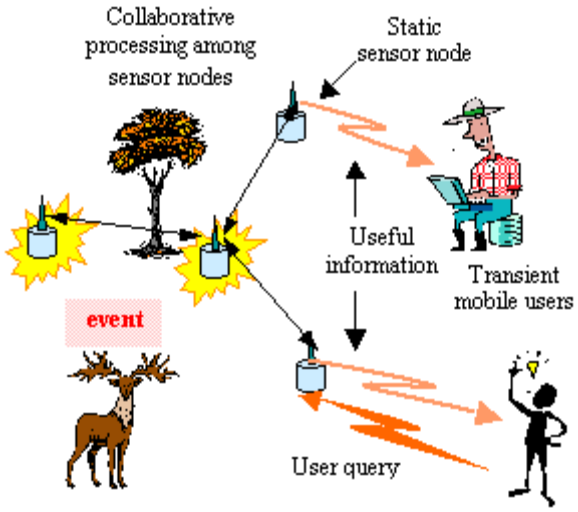

Figure 1: Distributed Sensor Networks

They are open to different varieties of attacks, including node capture and denial of service and tampering physically, promoting a range of fundamental research challenges. In DSNs, the primary challenges of sensor networks are by two facts. First, sensors are extremely energy constrained. Secondly, in most of the applications nodes will be randomly deployed. This randomness leads to the issue of dimensioning the sensor network. The nodes deployed may be either in a controlled environment where monitoring, maintenance and surveillance are very difficult. In the uncontrolled environments, security for sensor networks becomes extremely important. Network hole appears in the network due to the destruction of group of nodes. Holes in networks often cause failures in message routing due to the local minimum problem. Therefore, traditional geographic routing protocols cannot be applied with such topology management protocols.

1.1 Security Threats and Issues in Distributed Sensor Networks (DSNs)

There are several security requirements to guard a network.

1.1.1 Denial of Service (DoS)

A Denial of Service attack in sensor networks in general is defined as any event that eliminates the network's capacity

to perform its desired function. DoS attacks in distributed sensor networks may be carried out at different layers like the physical, link, routing and transport layers. This occurs by the unintentional failure of sensor nodes. The simplest DoS attack tries to exhaust the resources available to the victim node, by transmitting additional unwanted packets and thus prevents legitimate sensor network users from tapping work or resources to which these nodes are deployed. In DSNs, several types of Denial of Service attacks in different layers might be performed, i.e. at physical layer, the Denial of Service attacks could be jamming and tampering, at link layer, collision, exhaustion, unfairness, at network layer, neglect and greed, homing, misdirection, black holes and at transport layer this attack could be performed by malicious flooding and resynchronizations.

1.1.2 Hello flood attack

In this, HELLO packets will have high radio transmission range and these are used as weapons in DSN. This processing power sends HELLO packets to a number of sensor nodes, which are deployed, in a large area within a Sensor Network. The sensor devices are thus persuaded that the adversary is their neighboring node. As a result of this, while forwarding the messages to the base station, the victim sensor nodes try to go through the attacker as they are aware, that it is their neigh borers and are spoofed by the attacker.

1.1.3Wormhole attacks

In wormhole attack (Figure2), more than two malicious colluding sensor nodes does a virtual tunnel in the sensor network, which is used to forward message packets between the tunnel edge points. This tunnel establishes shorter links in the networkin which adversary documents forwards packets at one location in the sensor network, tunnels them to different location, and re-forwards them into the sensor network. In sensor network when sender node sends a message to another receiver node in the network, then the receiving node tries to send the message to its neighboring nodes. The neighbor sensor nodes assume that the message was sent by the sender node (this is normally out of range), so they tries to forward the message to the originating node, but this message never comes because it is too far away. Wormhole attack is a great threat to sensor networks since, this type of attack will not require compromising a sensor in the network instead; it could be performed even at the starting phase during the sensors initializes to identify its neighboring information. This Wormhole attacks are very difficult to stop since routing information given by a sensor node is very difficult to check. The wormhole attack is possible even when the attacker has not compromised with any hosts nodes and even if all communication provides confidentiality and are authenticated also.

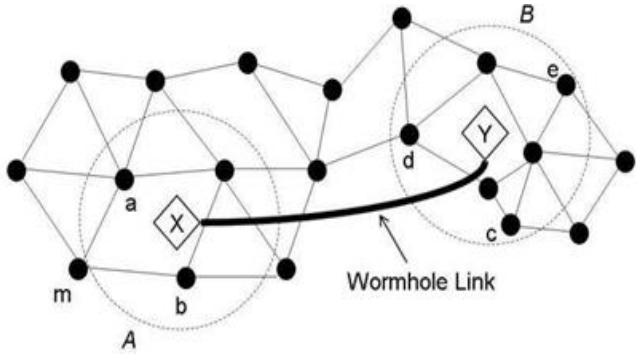

Figure 2: Wormhole Attack

1.1.3.1 Classification of Wormhole Attacks

In a wormhole attack two partners work together. One receives the packets, tunnels the packets to its partner and then the partner replays them into the network. Wormhole attack may be hidden or exposed type. In hidden wormhole attack malicious nodes hide the fact that they are involved in packet transmission i.e., legitimate nodes do not know about their existence. In exposed wormhole attack legitimate nodes know the participation of malicious nodes in packet forwarding but not aware that they are malicious.

1) Hidden Attack

The attacker does not modify the content of packet and packet header, even if the packet is an AODV advertisement packet. Instead, they simply tunnel the packet from one point and replay them at another point. This type of attack gives an illusion that sender and receiver are one hop neighbors. In fig(a), sender forwards the packet, which is received by M1. M1 does not modify the packet header, tunnels it as it is to M2. M2 replays the packet to R without modifying packet header. So S believes that R is its immediate neighbor and route is set up as {S, R}.

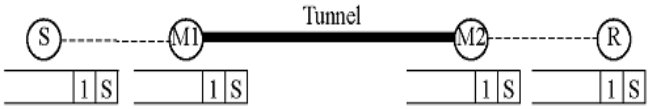

Figure 3: Hidden Attack

2) Exposed Attack

In this kind of attack, the attacker does not modify the content of the packet, but include themselves into the packet header following the route setup procedure as shown in fig (b). S forwards the packet to M1; M1 finds the previous hop value as 1, update it as 2 and forwards the packet to M2. M2 finds previous hop count as 2, update it as 3 and replays the packet to R. Hence the route is set up as {S, M1, M2, R}.
In both kinds of attack, there is at least one pair of neighbors that are not actually direct neighbors and they are referred to as “false neighbors”.

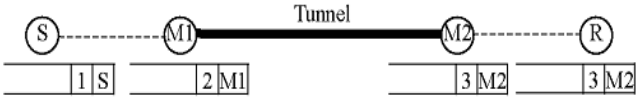

Figure 4: Exposed Attack

Wormhole attacks can be further classified on the basis of:
a) Its Implementation
b) The medium used
c) The attackers

d) The location of victim nodes.

a) Classification based upon Implementation
This is the most important classification; whichdepends upon the behavior the attack is launched.

i. Using Encapsulation:
In this manner, there are some nodes which areoccupied along the path (these nodes may or may notbe conscious of wormhole) between S and R. Thepacket gets encapsulated at S and travels through thepath in encapsulated form to avoid the increase in thehop count. In this case the attackers are not directlyconnected to one another rather make the other nodesbelieve that they are directly connected. These packetsare transmitted between S and R using a virtual tunnel. Once this attack is successfully launched, then all thepaths will contain a link that will contain of link betweenS and R.

ii. Using Out-Of-Band Channel
These colluder nodes get connected directlythrough a out of band channel having high bandwidth.The channel can be obtained by a wired connection orusing a wireless connections. The requirement of extrahardware made it difficult to launch, but provides asimplicity because it will not require anyencapsulation/de-capsulation while the colluders aredirectly connected.

iii. Using High Power Transmission
This type of wormhole particularly launchedfrom two colluder nodes that facilitates high powertransmission potential.

iv. Via Protocol Deviations
In this case the attackers generate thewormhole by not following the protocol set of laws e.g.Some protocols suppose the nodes to wait for a whilebefore retransmitting but the attackers keeps onbroadcasting and do not obey this rule and thus tryingto reach first at the destination and thus avoiding anyfuture genuine requests to reach destination. If the futurerequests arrive at destination, they will be dropped,since a request passing through the colluder haspreviously been received.

b) Classification based upon Medium Used
On the basis of medium used, wormholeattacks can be classified as in-band and out-of-bandwormhole attacks.

i. In-Band Wormhole
Same medium will be used by the attackers forcreating link between them e.g. protocol deviations,packet relay and, encapsulation.

ii. Out-Of-Band Wormhole
Like normal network nodes attackers do not usethe same medium, e.g. High Transmission Mode andOut-Of-Band Channel.

c) Classification based upon Attackers
i. Self-Sufficient
Here colluder nodes present themselves asnormal nodes and thus all paths passes through theme.g. using high power transmission or out-of-bandchannel.

ii. Extended Wormhole
The colluder nodes extends the attacks beyondthemselves to normal nodes and are unseen bythemselves e.g. packet relay or encapsulation.

d) Classification based upon location of Victim nodes
i. Simplex
The victim node is present inside the range ofonly one attacker.
ii. Duplex
The victim node is present inside the range ofboth the attackers.

We address the wormhole attack, which is a ruthless attack in distributed sensor networks whereby an attacker stores transmitted packets and then replays them into the network. A typical wormhole attack requires two or more attackers - malicious nodes - who have better communication resources than regular sensor nodes. The attacker creates a low-latency link (i.e. high-bandwidth tunnel) between two or more attackers in the network. Attackers promote these tunnels as high-quality routes to the base station. Hence, neighboring sensor nodes adopt these tunnels into their communication paths, rendering their data under the scrutiny of the adversaries. Once the tunnel is established, the attacker collect data packets on one end of the tunnel, sends them using the tunnel (wired or wireless links) and replays them at other end Wormhole attacks may result in serious damages in DSNs by interrupting or altering the information flow towards the base station. In addition, if the attackers do not modify or fabricate data packets, cryptographic solutions alone cannot detect wormhole attacks. Defending against such an attack is challenging because it can be launched even if all network communication is authentic and confidential.

2. Literature Review

In [1], [2] & [3] authors have discussed different varieties of attacks in sensor networks, including node capture and denial of service and tampering physically. In [4],[5],[6] and [12]the authors have presented a security solution framework prepared to the base station to defend against Denial of Service (DoS) attack. The DoS attack is meant that normally attempt to disrupt or destroy a network, and it also diminishes a network's capability to provide a service. In [7] & [8] authors discusses the wormhole attack. In [9], authors proposed a solution to wormhole attacks for wireless sensor adhoc networks in which all sensor nodes are equipped by *directional antennas*. In these method nodes utilizes predefined sectors of their antennas to communicate with one another. Each pair of sensor nodes has to check the direction of received message signals by its neighboring sensor node. Thereby, the neighbor relation is established only when the directions of both couples are matched. This additional informationmakes wormhole discovery and intern introduces great amount of inconsistencies in the sensor network, and this can be easily be detected. Wang and Bhargava [10] propose a methodology in which sensor network visualization is employed for the detection of wormhole attacks in stationary wireless sensor networks. In this presentation, each sensor node calculates the distance to its neighbors based on signal strength received. Each and

every sensor informs this distance data to the central controller, which studies the sensor network's physical *topology* depending upon every sensor node distance measurements. Without presence of wormholes, the sensor network topology should be almost flat, whereas a wormhole would be observed as a string stretching different ends of the wireless sensor network together.

Song et al [11] presents a wormhole discovery mechanism, which is depending on *statistical analysis* of multipath routing. Song noted that a link established by a wormhole is attractive in routing sense, and this will be selected and requested with very high frequency as it only uses routing information, which is already available to a sensor node. Hu et al. [16] proposed the method in 2003based upon *geographical and temporal packet leaches*.In this method to avoid the wormhole, the geographicallocation or temporal location is used to bound thedistance travelled by the packet. This approach isrestricted by condition of GPS technology or the timesynchronization. Lazos et al. [17] proposed a method in2005 where a few nodes are mandatory to be equippedby GPS locators and directional antennas. Thisprocedure uses *"local broadcast keys"* for safecommunication between one another.Tran et al. and Phuong et al. proposed *TTM*(Transmission Time based Mechanism) in 2007, whereevery node in the pathway work together and attack isidentified through route setup stage by calculatingtransmission time among two nodes. Venkataramanetal.in 2009 proposed a *graph theoretic mechanism* for the finding of wormhole attacks, which is right for proactive protocols.Chen et al. [18] proposed a secure localization approach in 2010 based on the inconsistent set based resistant localization. Graaf et al. [19] proposed a dispersed detection approach based upon ranges of nodes for the detection of wormhole attacks. A Vani et al. [20] proposed a solution in 2011 that combines the decision anomaly, neighbor list count and hop count methods for AODV protocol. This procedure depends upon hierarchical processing of nodes and their respective neighbors. They used the hop count information available in the routing table of the nodes which needs that we need to store two copies of routing table of every node so as to maintain the track of earlier hop counts.

In [22] simulation results based on packet reception ratio, packet dropped ratio, and throughput and providing higher level security is presented. Routing attack for wireless sensor network and can be implemented by using Mint route protocol to defend against.[23] In this paper alternative path from source to second hop and calculate the number of hops todetect the wormhole. The technique is localized, requires only a small overhead, and does nothave special requirements such as location information, accurate synchronization between nodes. In WORMEROS [33], two phases are used to detect wormhole in the network. First phase is *Suspicion phase* where RTT between a node *S* and all of its immediate neighbors is measured. If RTT(*S,D*), where *D* is one of *S*'s neighbors, is abnormally higher than the average RTT of all links from *S* to its neighbors, then there might be a wormhole between *S* and *D*. This technique does not require the cooperation of all nodes in the path between Sand *D*. Second, it uses an observation that in a dense network, two neighbors *S* and *D* are likely to share some common neighbors. This technique uses only local information instead of global information. If any of the techniques in the Suspicion phase detects the existence of a suspicious link, then second phase of WORMEROS is executed to confirm the wormhole.The second phase of WORMEROS is *Confirmation phase* where it launches a series of challenges to make sure that the wormhole is correctly identified. In this phase, the two legitimate nodes being attacked by the wormhole link collaborate to challenge the attacker. Frequency hopping can be used for this purpose. The proposed method is energy efficient as advanced techniques in the second phase are applied only when the wormhole attack is suspected.The major drawback of this work is that topological change is not considered.In [35], Farid et al, proposed wormhole detection and prevention techniques against OLSR protocol. In the wormhole detection phase, wormhole link is suspected based on the average propagation delay of HELLO message. As this delay is influenced by many other parameters like congestion, intra nodal processing and so on, the proposed work defines two new control packets HELLO*req*and HELLO*rep*for OLSR protocol.The major drawback of this proposed system is that mobility is not considered and false detection is not handled.

In [36] DelPHI (Delay Per Hop Indication) wormhole detection mechanism consists of two phases. First is *Data Collection phase* in which two messages DREQ and DREP are used similar to AODV RREQ and RREP to find the disjoint paths to the receiver and message back to the sender to identify paths respectively. Both DREQ and DREP include previous hop field, hop count field and a time stamp field. Receiver replies to each DREQ packet received and each node broadcasts DREQ only once. Using the previous hop field, hop count is incremented by 1 upon receiving the DREP packet. Also time stamp is used to compare the RTTs. To ensure reliability data collection phase is repeated thrice.Second is *Data Analysis and Detection phase* in which RTT is calculated. RTT for normal path remains same whereas for wormhole paths, the RTT will be larger but the hop count remains same.Advantages of this method are they do not require clock synchronization; position information and mobile nodes need not to be equipped with special hardware and thus provides power efficiency. The message overhead of DelPHI in providing reliability is a tradeoff between the two parameters and needs further investigation. False detection is also not handled.In [39] DaW (Defense against Wormhole), wormhole security model, monitoring nodes, calculation of trust and wormhole detection are discussed. Wormhole detection is carried out in the following sequence.

- Broadcast RREQ
- Append trust vectors
- Send RREP
- Check for suspicious link
- Confirm wormhole

This proposed mechanism does not handle false detection efficiently and mobility of the network is not considered.To the best of our knowledge mobility of nodes is not handled efficiently by most of the proposed mechanisms. So, we are working in that direction to achieve wormhole detection, localization and mitigation techniques in mobile wireless networks.

3. Objectives

Objectives of the research are to design a framework to detect, locate, mitigate and prevent the wormhole attacks in distributed wireless sensor networks.

- To design a novel architecture to discover the wormhole attacks in dynamic (mobile) wireless sensor networks. The approach should have high fault tolerance and fault detection rates.
- To design a scheme to dynamically and automatically locate the wormhole attacks.
- To develop a mechanism and in turn develop a novel algorithm to mitigate wormhole attacks using a distributed approach.

4. Methods

Our research proposal aims at providing the secure platform for distributed wireless sensor networks to automatically identify the wormhole attacks and mitigating this problem.

4.1 Discovery of wormhole attack in wireless sensor networks

Wormhole attacks basically cause the problem to the route discovery mechanism in distributed wireless sensor networks. In a wormhole attack, the malicious nodes will tunnel the eavesdropped packets to a remote position in the network and retransmit them to generate fake neighbor connections, thus spoiling the routing protocols and weakening some security enhancements. To the best of our knowledge, the existing mechanisms to detect wormhole attacks in wireless sensor networks fail to eliminate wormhole from the networks efficiently. Hence in our proposed research work, we have planned to make use of graph theory for characterizing the wormhole attack and derive the necessary and sufficient conditions for any candidate solution to prevent wormholes. In the proposed graph theory based solution, we will make use of time bound based method like computation of *round trip time or neighbor numbers based wormhole detection mechanism*. The proposed scheme/mechanism is planned to simulate using network simulation tool. To prove the performance efficiency of our proposed method, we will compare and analyze the simulation results with the existing standard approaches.

4.1.1 Proposed wormhole detection mechanism

In this section we present our wormhole detection mechanism based on the calculation of Round Trip Time (RTT) and neighbor number based. Our proposed system does not require any special hardware or synchronized clocks because we only consider its local clock to calculate the RTT.Our detection is based on the calculation of RTT of the message between nodes. We depict that existence of wormhole nodes may lead to larger RTT value between successive nodes. But larger RTT alone is not a sufficient condition to detect wormhole, because other factors like network congestion, intra node processing may also result in larger RTT value. So, neighbor number testing phase is included to confirm and pinpoint the location of wormhole.
Various phases associated with wormhole detection are:

- Route discovery
- RTT calculation
- Wormhole Attack Detection
- Neighbor number list
- Evaluation

Route Discovery

AODV is a reactive or on demand protocol which discovers routes as and when necessary and does not maintain routes from every node to every other node. Routes are maintained just as long as necessary and every node maintain its monotonically increasing sequence number which increases every time when it notices change in the neighborhood topology. When a node wishes to send a packet to a destination, it checks its routing table to determine if it has a current route to the destination. If yes, forwards the packet to the next hop node otherwise initiates a route discovery process.

Route discovery process begins with the creation of Route Request (R_{REQ}) packet created by sender. The sender sends the R_{REQ}message to the neighbor node and saves the time of its R_{REQ} sending T_{REQ}. The intermediate node also forwards the R_{REQ}message and save T_{REQ} of its sending time. When the R_{REQ} message reach to the destination node, it reply Route Reply message (R_{REP}) with the reversed path. When the intermediate nodes receive the R_{REP} message, it saves the time of receiving of R_{REP} T*REP*. Our assumption is based on the RTT of the route request and reply. The RTT can be calculated as

$$RTT = T_{REP}-T_{REQ} \quad \ldots\ldots\ldots\ldots (1)$$

All intermediate nodes save this information and then send it also to the base station.

RTT calculation

The round-trip travel time i.e. RTT of a message and the distance between the nodes based on this travel time is calculated. To calculate RTT, every node will have two time stamps, which store

i. Forwarding time of the request from source to destination (R_{REQ})
ii. Receiving time of the reply to source back (R_{REP})

Given all RTT values between nodes in the route and the destination, RTT between two successive nodes, say A and B can be calculated as follows:

$$RTT_{A,B} = RTT_A - RTT_B \quad \ldots\ldots\ldots\ldots\ldots (2)$$

Where RTT_A is the RTT between node A and the destination and RTT_B is the RTT between node B and destination. The route from source S to receiver R pass through node M1 and M2, so routing path includes, S→ M1→ M2→ R. Then the RTT between S, M1, M2 and M3 is calculated based on equation (1) as followed:

$$RTT_S = T(S)_{REP} - T(S)_{REQ}$$
$$RTT_{M1} = T(M1)_{REP} - T(M1)_{REQ}$$
$$RTT_{M2} = T(M2)_{REP} - T(M2)_{REQ}$$
$$RTT_R = T(R)_{REP} - T(R)_{REQ}$$

And the RTT values between two successive nodes along the path will be calculated based on equation (2):

$$RTT_{S,M1} = RTT_S - RTT_{M1}$$
$$RTT_{M1,M2} = RTT_{M1} - RTT_{M2}$$
$$RTT_{M2,R} = RTT_{M2} - RTT_R$$

The values of $RTT_{S, M1,}$ $RTT_{M2, R,}$ $RTT_{M1, M2}$ are almost in the same range in the absence of wormhole attack. If there is a wormhole link existing between a pair of nodes then RTT value is considerably larger than other successive RTT values.

Wormhole Attack Detection

When the source node gets RREP, it initiates wormhole detection mechanism.RTT between pairs of nodes is calculated and it is compared with RTT of all other pairs of nodes. Under normal circumstances, RTT value for all pairs of nodes is in the same range. Suppose, if there is considerable amount of increase in RTT then we suspect that there is a wormhole link. A threshold value has been set for RTT to detect the presence of wormhole attack taking into account network congestion, intra nodal processing and so on.

Neighbor Number List

When the network is deployed, each node identifies its neighbors and maintains the list of the same using suitable protocol. If the RTT value is considerably higher than the average RTT values of successive nodes, then there may be wormhole link. To confirm that, new links are introduced into the network. The attacker tries to increase the number of neighbor nodes (nn) within its radius. The suspected node's neighboring nodes are also checked to estimate average number of neighbors N, which is given as

$$N= (n-1)\ \pi\ r^2/P \quad \ldots\ldots\ldots\ldots\ldots\ (3)$$

Where,

P→ area of the network region

n→ number of nodes in that region

r→ common transmission radius.

Suspected node pair's 'N' is calculated and if **nn> N** then wormhole link is detected between node pairs.

Evaluation

The performance of proposed system is evaluated using network simulator (NS2). Performance metrics **like Throughput, Energy Consumption, and Packet Delivery Ratio (PDR)** are calculated.

4.2 Dynamic and automatic location of wormhole attacks in wireless sensor networks

In wireless sensor network, wormhole attack sniffs packets at some point and passes them through wireless link to another point. This causes severe influence on the localization process. In our research proposal, to locate automatically and dynamically, we have planned to adapt the methodology based on *game theory or artificial intelligence technique*. Initially, we analyze the impact of the wormhole attack on the localization in wireless sensor networks and finally we propose a wormhole attack resistant secure localization scheme. The methodology to provide wormhole attack resistant secure localization scheme is to build an intelligent conflictions for message exchanges among neighboring nodes, and then to identify all dubious locators, which are filtered out during localization. This scheme may provide high probability secure localization. To validate the proposed scheme we planned to simulate using network simulators by comparing with the existing schemes under different network parameters.

4.3 Mitigation of wormhole attacks in wireless sensor networks

Basically in wormhole attack, a malicious node in wireless sensor network records control traffic at one location and tunnels it tofar away from node, which replays it locally. This can have an adverse effect on route establishment by preventing nodes from discovering legitimate routes that are more than two hops away. Hence in this research proposal, we have planned to address the issue of mitigation of wormhole attack in wireless sensor network based on certain authentication mechanisms. The proposed architecture will be based on two-tier. In first tier local monitoring technique may be applied to detect and isolate malicious nodes locally. In second tier, we develop a secure central authority for global tracking of node positions. When a strong suspicion builds at central authority in second tier, it enforces a global isolation of the malicious node from the whole network. This mitigation problem will be analyzed through extensive simulation using network simulators by comparing with the existing standard approaches.

5. Results and Discussions

Fig.5 shows as the number of interval increases throughput decreases exponentially. Throughput for proposed method is 7-10% better than throughput without detection mechanism.Fig.6 shows the average energy consumption v/s number of interval. Average energy consumption for proposed mechanism is 5% more efficient.

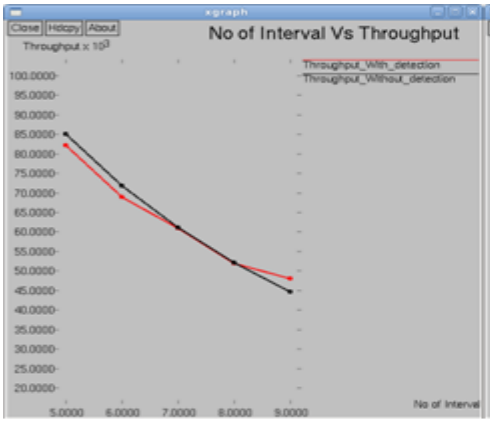

Figure 5: No. of Interval vs. Throughput

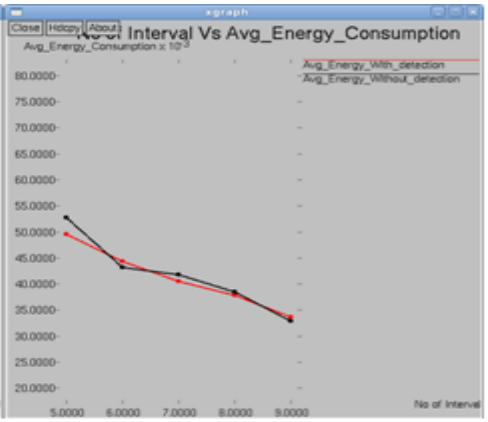

Figure 6: No. of Interval vs. Average Energy Consumption

Fig.7 shows as number of interval increases PDR decreases gradually. PDR of proposed method is 8% better.

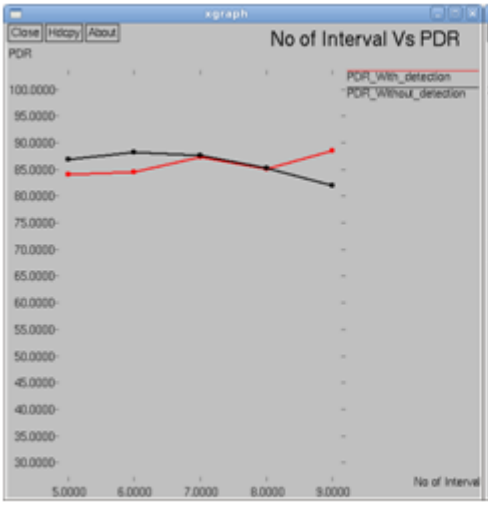

Figure 7: No. of Interval vs. PDR

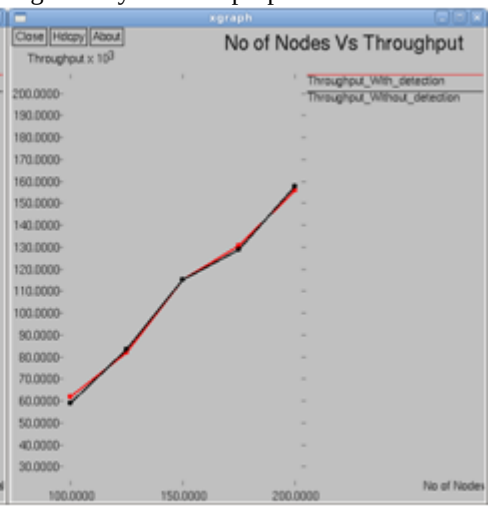

Figure 8: No. of Nodes vs. Throughput

Fig.8 shows as the number of nodes increases throughput increases. Fig 9.showsas the number of nodes increases average energy consumption increases and has to be addressed in the future work.

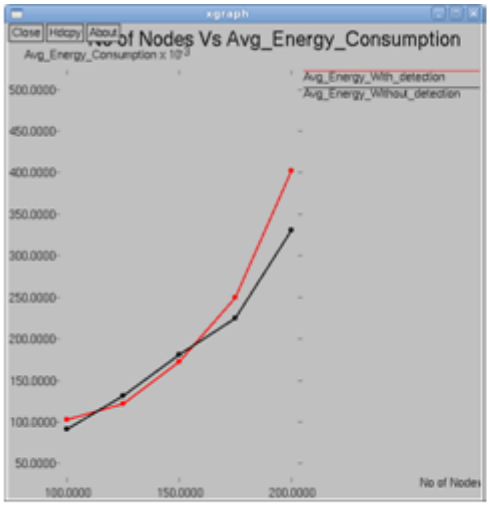

Figure 9: No. of Nodes vs. Average Energy Consumption

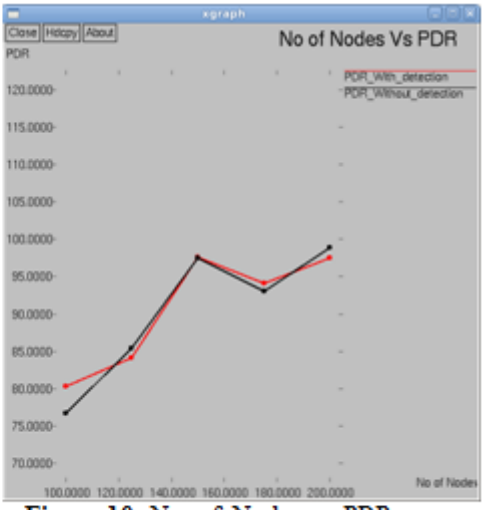

Figure 10: No. of Nodes vs. PDR

Fig. 10 shows as the number of nodes increases PDR also increases. Fig 11 and 12 shows the variation of Packet size v/s throughput and packet size v/s average energy consumption respectively.

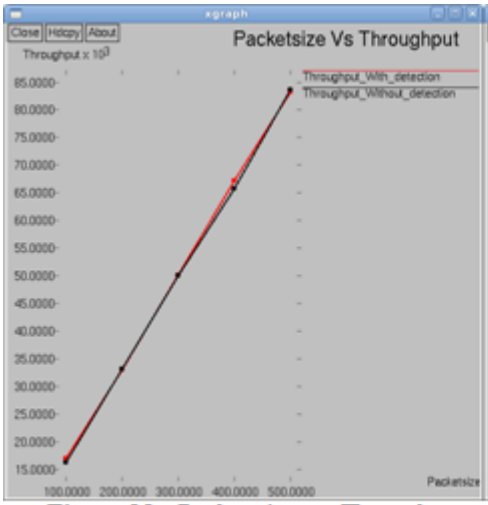

Figure 11: Packet size vs. Throughput Energy Consumption

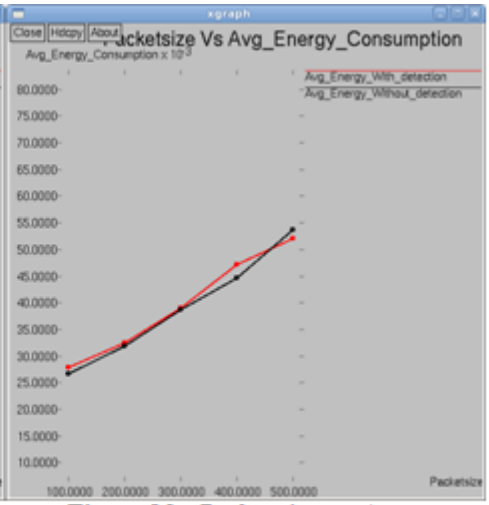

Figure 12: Packet size vs. Average

6. Conclusion

Defending against wormhole attack is crucial to the viability of sensor network deployments. Providing such security is critical if sensor networks are to realize the promise of widespread deployment. We can overcome many threats and attacks on wireless sensor networks using our proposed mechanisms for wormhole issue. Our proposed research solutions in wireless sensor networks can alert network administrators of ongoing attacks or trigger techniques to conserve energy on affected devices. Such mechanisms complement current authentication techniques and would help prevent many of the attacks. Our research proposal provides add on service for the secure platform of wireless sensor networks without increasing the hardware complexity.

7. Future Scope

In our proposed work, we have dealt with graph theory based wormhole detection mechanism only. Remaining objectives of our research work is to propose mechanisms to automatically locate and mitigate wormhole attacks in mobile wireless sensor networks using game theory/ artificial intelligence techniques and two tier authentication mechanisms respectively.

References

[1] Adrian Perrig, John Stankovic, and David Wagner," Security in wireless sensor networks". ACM Communication, 47(6): 2004, pp. 53-57.
[2] A.D. Wood and J.A. Stankovic, (2002) "Denial of Service in Sensor Networks," Computer, vol. 35, no. 10, 2002, pp. 54–62.
[3] David R. Raymond and Scott F. Midkiff, (2008) "Denial-of-Service in Wireless Sensor Networks: Attacks and Defenses," IEEE Pervasive Computing, vol. 7, no. 1, 2008, pp. 74-81.
[4] Zhen Cao, Xia Zhou, MaoxingXu, Zhong Chen, Jianbin Hu, Liyong Tang , "Enhancing Base Station Security against DoS Attacks in Wireless Sensor Networks", IEEE, 2006.
[5] J. Kong, Z. Ji, W. Wang, M. Gerla, R. Bagrodia and B. Bhargava" Lowcost attacks against packet delivery, localization and time synchronization services in underwater sensor networks", Proceedings of the Fourth ACM Workshop on Wireless Security, 2005, pp. 87-96.
[6] ZawTun and AungHtein Maw,(2008)," Worm hole Attack Detection in Wireless Sensor networks", proceedings of world Academy of Science, Engineering and Technology Volume 36, December 2008, ISSN 2070-3740.
[7] KhinSandar Win, Department of Engineering Physics, Mandalay Technological University, PatheinGyi, Mandalay," Analysis of Detecting Wormhole Attack in Wireless Networks", World Academy of Science, Engineering and Technology , 2008,pp.48-55
[8] L. Hu, D. Evans, Using Directional Antennas to Prevent Wormhole Attacks, 14 Proceedings of the 11th Network and Distributed System Security Symposium, pp. 2003.
[9] W. Wang, B. Bhargava., Visualization of wormholes in sensor networks, Proceedings of the 2004 ACM workshop on Wireless Security, pp. 51-60, 2004.
[10] I. Khalil, S. Bagchi, and N. B. Shroff, "LITEWORP: A Lightweight Countermeasure for the Wormhole attack in multihop wireless network," in International Conference on Dependable Systems and Networks (DSN), 2005.
[11] D.G.Anand, Dr.H.G.Chandrakanth, Dr.M.N.Giriprasad, "Security Threats & Issues In Wireless Sensor Networks", In International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 Vol. 2, Issue 1,Jan-Feb 2012, pp.911-916
[12] Akanksha Gupta &Anuj K. Gupta "A Survey: Detection and Prevention of Wormhole Attack in Wireless Sensor Networks" Global Journal of Computer Science and Technology: E Network, Web & Security Volume 14 Issue 1 Version 1.0 Year 2014. Online ISSN: 0975-4172 & Print ISSN: 0975-4350.
[13] MojtabaGhanaatpishehSanaei, BabakEmamiAbarghouei, HadiZamani, Miranda Dabiranzohouri "An Overview on Wormhole Attack Detection in Ad-Hoc Networks" Journal of Theoretical and Applied Information Technology 30th June 2013. Vol. 52 No.3 ISSN: 1992-8645 E-ISSN: 1817-3195.
[14] Ankita Gupta and Sanjay PrakashRanga "Wormhole Detection Methods in Manet" International Journal of Enterprise Computing and Business Systems (Online) IJECBS India Vol. 2 Issue 2 July 2012.
[15] A.BabuKaruppiah, G.Sri Vidhya, S.Rajaram "An Energy Efficient Wormhole Detection Technique by Traffic Analysis in Wireless Sensor Networks "International Journal Of Engineering And Computer Science ISSN:2319-7242 Volume 2 Issue 2 Feb 2013 Page No. 311-316.
[16] Hu, Y.-C.; Perrig, A.; Johnson, D.B.; "Packet leashes: a defense against wormhole attacks in wireless networks,". Twenty-Second Annual Joint Conference of the IEEE Computer and Communications. Lazos, L.; Poovendran, R.; Syverson, P.; Chang,
[17] L.W.; "Preventing wormhole attacks on wireless ad hoc networks: a graph theoretic approach," Wireless Communications and Networking Conference, March 2005.IEEE Societies , April 2003.
[18] Honglong Chen , Wei Lou , Zhi Wang, A secure localization approach against wormhole attacks using distance consistency, EURASIP Journal on Wireless Communications and Networking, April 2010.
[19] R. Graaf, I. Hegazy, J. Horton. "Detection of wormhole attacks in wireless sensor networks," Springer book chapter Ad Hoc Networks, 2010.
[20] A.Vani, D. SreenivasaRao, "A Simple Algorithm for Detection and Removal of Wormhole Attacks for Secure Routing In Ad Hoc Wireless Networks", International Journal on Computer Science and Engineering (IJCSE), June 2011.
[21] BintuKadhiwala and Harsh Shah, "Exploration of Wormhole Attack with its Detection and Prevention Techniques in Wireless Ad-hoc Networks", International Conference in Recent Trends in Information Technology and Computer Science (ICRTITCS - 2012) Proceedings published in

International Journal of Computer Applications (IJCA) (0975 – 8887).

[22] Kashyap Patel and T .Manoranjitham, "Detection of Wormhole attack in wireless sensor network"International Journal of Engineering Research & Technology (IJERT) ISSN: 2278-0181, Vol. 2 Issue 5, May -2013.

[23] [13] Devendra Singh, KushwahaAshishKhare, J. L .Rana, "Improved Trustful Routing Protocol to Detect Wormhole Attack in MANET" International Journal of Computer Applications (0975 – 8887), Volume 62– No.7, January 2013

[24] PriyaMaidamwar and NekitaChavhan "Survey on Security Issues to Detect Wormhole Attack In Wireless Sensor Network" International Journal on AdHoc Networking Systems (IJANS) Vol. 2, No. 4, October 2012 DOI : 10.5121/ijans.2012.2404 37 A .

[25] Manisha, Gaurav Gupta, NiveditaKashyap, RuchikaChandel, , Vandana Sharma "A Qualitative Comparative Study: Wormhole Attack Detection Techniques in WSN at Network Layer" International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online) Vol. 2, Issue 2, pp: (325-331), Month: April-June 2014.

[26] MajidMeghdadi, SuatOzdemir and InanGüler"A Survey of Wormhole-based Attacks and their Countermeasures in Wireless Sensor Networks"IETE TECHNICAL REVIEW | VOL 28 | ISSUE 2 | MAR-APR 2011.

[27] Ahmad Heidari"A Survey of Wormhole Attack and Countermeasures against that in Wireless Ad-hoc Networks" 5thSASTech 2011, Khavaran Higher-education Institute, Mashhad, Iran. May 12-14.

[28] HarleenKaur, Neetu Gupta "Detecting Wormhole Nodes in WSN using Data Trackers" International Journal of Engineering Research and General Science Volume 2, Issue 4, June-July, 2014 ISSN 2091-2730 288.

[29] Bipin N. Patel, Prof. Tushar S. Patel "A Survey on Detecting Wormhole Attack in Manet" International Journal of Engineering Research and Applications ISSN : 2248-9622, Vol. 4, Issue 3(Version 1), March 2014, pp.653-656.

[30] Rajpal Singh Khainwar, Mr. Anurag Jain, Mr. Jagdish Prasad Tyagi"Elimination of Wormhole Attacker Node in MANET using Performance Evaluation Multipath Algorithm" International Journal of Emerging Technology and Advanced Engineering (ISSN 2250-2459,Volume 1, Issue 2, December 2011)

[31] Nishant Sharma, Upinderpal Sing2 "Various Approaches to Detect Wormhole Attack in Wireless Sensor Networks "IJCSMC, Vol. 3, Issue. 2, February 2014, pg.29 – 33

[32] Moutushi Singh, Rupayan Das "A Survey of Different Techniques for Detection of Wormhole Attack in Wireless Sensor Network "International Journal of Scientific & Engineering Research Volume 3, Issue 10, October-2012 1ISSN 2229-5518 IJSER © 2012 http://www .ijser.org.

[33] 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 Conference on Wireless Algorithms Systems and Applications, 2008.

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

[35] F. Nait-Abdesselam, B. Bensaou. "Detecting and Avoiding Wormhole Attacks in Wireless Ad hoc Networks", IEEE Communications Magazine, 2008.

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

[37] 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, 2005.

[38] M.S. Sankaran, 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.

[39] KhinSandar Win. "Analysis of Detecting Wormhole Attack in Wireless Networks", World Academy of Science, Engineering and Technology, 2008.

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