Journal of Communications Technology, Electronics and Computer Science, Issue 16, 2018
ISSN 2457-905X

Implementation of Information Systems Security Threats: The Byzantine Generals and Wormhole Attacks

Nancy Alrajei

Palestine Polytechnic University, Department of Information Systems and Multimedia, Rochester, Hebron, Palestine

Abstract—A challenge in designing wireless sensor networks is to maximize the lifetime of the network with respect to limited resources and energy. These limitations make the network particularly vulnerable to attacks from adversaries. Attacks such as wormhole attack and Byzantine General Attack, that are considered damaging to the security of the information system of the network. In this paper we implemented those two attacks on different network settings and topologies to test how it affects the information that is being spread in the network in the presence of these attacks. We use Matlab simulation and our results show the differences between the between different topologies on the stability of the information of the network.

Keywords—security, Byzantine General, wormhole, attacks, Information Systems, wireless network, network topology.

I. INTRODUCTION

Wireless sensor networks (WSN) consist of individual nodes that are able to perceive their environment, communicate with nearby nodes via radio broadcast, and perform computations based on information gathered from their surroundings. The main goal of such network is to perform distributed sensing tasks for applications, such as environmental mentoring. The deployment of sensor network in hostile environments, combined with limitations of the sensors, limited power, and memory and computation resources makes them vulnerable to variety of attacks.

The network lifetime is the time span from the deployment to the instant when the network is considered non-functional. Once these sensors are deployed, it is almost impossible to conduct regular maintenance. Due to the fact that network may consist of a very large number of nodes or the nodes may be in an environment in which human intervention is difficult or undesirable.

The wireless sensor network is vulnerable to attacks due to its limitations and lack of structure. Those attacks can target the following security requirements:

(A) *Confidentiality*: impedes access of unauthorized people to obtain data which is one of the crucial requirements in sensitive WSN applications. A sensor node should not relay on the data derived from the environment to its neighbors. The data collected on the nodes can be very sensitive, particularly in military applications. Furthermore, in numerous applications, nodes have to transmit highly sensitive data to other sensor nodes by means of wireless transmission environment such as routing data. Malicious nodes because these nodes can exploit these data and reduce the performance of the network.

(B) *Data Authentication*: Since WSNs use public wireless environment, they need authentication mechanisms to pick up messages and deceptive packets that come from malicious nodes. Authentication mechanisms aid a node in verifying the identity of a node that it is in contact with. If there is no authentication, a malicious node can behave as if it was a different node and might acquire some sensitive data and also hamper proper operation of other nodes. In case only two nodes are in contact, authentication can be achieved by symmetric key cryptography. Transmitter and receiver can compute the verification code of all the messages sent by a common hidden key.

(C) *Data Freshness*: In WSN structures, sensors send measurement data related to environment in which they are present through specific time intervals and then what matters is the delivery of the measurement times. It is possible that an attacker can retransmit the copy of old measurement values. It is therefore important to check that the data is new.

(D) *Availability*: WSN’s capability in sustaining its service continuity even during denial-of service DoS attacks. Excessive communication or calculation load might run out of the battery of the node faster than expected. Highly serious consequences might result from not providing availability to WSN. Let us take a military based application as an example, if some nodes do not function properly, then the enemy alliances might leak from these nonfunctional parts of WSN. Developing a detection and defense unit is essential to provide availability

(E) *Data Integrity:* ensures that the message will not be altered during communication.

Examples of attacks that violates the previous security measures are Byzantine General attack and wormhole attack. A Byzantine node is a node that behaves in an arbitrary manner, or even according to some malicious design. It might send, to different destinations, different messages that purport to be the same message. Furthermore, Byzantine nodes might collaborate in an attempt to bring the system down. In fact, even if a bug eventually results in a crash, the system could have performed erroneous operations (and exhibited Byzantine behavior) between the original occurrence of the bug and the eventual crash. Such faulty behavior is hard to mask because it is difficult to tell if any node was performing correctly or not.

In wormhole attack, the attacker can forward each packet using wormhole links and without modifies the packet transmission by routing it to an unauthorized remote node. Hence, receiving the rebroadcast packets by the attackers, some nodes will have the illusion that they are close to the attacker. With the ability of changing network topologies and bypassing packets for further manipulation, wormhole attackers pose a severe threat to many functions in the network, such as routing and localization [3], [4], [5], [6], [7]

In this paper we implemented two of the failure attacks on wireless sensor network and tested if the topology affects how fast we detect the intruders, our results show different findings for same setting networks but with different topologies. We will explain this concept in details and show how we implemented the failure models.

paper is organized as follows. In Section 2 we present the background on the concepts that were adopted in this paper. Next. In Section 3, we explained the failure models then in Section 4 we implemented these models via simulation. In Section 5 we evaluated the results. Finally, we conclude in Section 6

II. Background

In our paper we have adopted the following approaches and concepts:

A. Gossip Protocol and its Variants

Gossip protocol is used for communication with neighbors in which nodes attempt to exchange rumors (message)[7],[8]. Variants of this problem have been well-studied in (synchronous) single-channel radio networks. There is a parameterized version of the gossip problem, called ϵ-gossip, in which (1 − ϵ) n rumors must be disseminated to at least n−1 nodes. As it is impossible to disseminate even a single value to all n receivers in this setting. The ϵ-gossip problem is a generalization of classical all-to-all gossip (0-gossip) that allows for flexibility in the number of rumors that need to be spread—a desirable feature for many applications (e.g., when only a majority vote is needed).We have used general gossip protocol as stated in [7] for communicating to its neighbors (criteria for being a neighbor is different for different network as stated above).

B. Push-Pull Communications Model

We have adopted push-based as well as pull-based model for our implementation. When data is pushed to the intended node based on some criteria, is termed as push-based schemes. When data is provided based on the request made by the user, is termed as pull-based scheme.

In our case, when any node is searching for higher version of patch to its immediate neighbors using gossip protocol, it gets patch if it finds higher patch. Otherwise it pushes its own patch to that neighbors which has lower version of patch. This way patches propagate throughout the network until it gets stabilized.

C. Network Topology

Network topology is how the sensor nodes are deployed on the area on interest. Sensors have limited range around them on which they can communicate with other nodes, this range is called the communication disk. A node can communicate with any node that is placed within its communication disk.

1) Mesh Topology

Neighboring nodes are adjacent through one edge on all directions, so it is represents a one hop routing network. In this topology, each node has 2-4 neighbors depending upon its location. Corner nodes have 2 neighbors, middle nodes have 3 neighbors and interior nodes have four neighbors. All nodes only communicate to only their direct neighbors. We assign a node such as in figure 3 Node 6 is a security patch server (base-station) in this network which maintains all the updates related to security software.

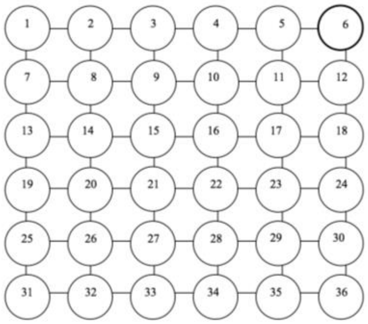

Figure 1. Mesh Network

2) Random Network:

This topology is inspired from sensor network architecture, where big number of sensors are being scattered randomly on the area of interest to monitor some phenomena. The randomness comes from 2 factors:

1. it is almost impossible to place sensor nodes by hand in large geographical area. So it is better to throw them randomly.
2. we never know where the attack will take place so it is better to cover the area with sensors that are randomly scattered and then we might, move nodes accordingly.

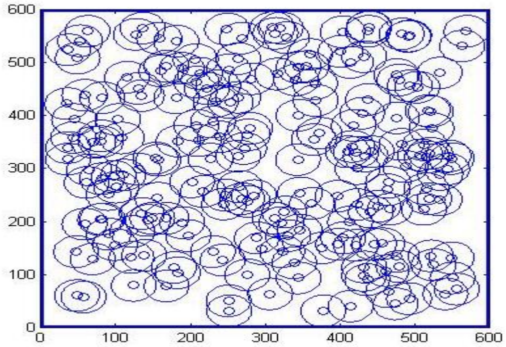

Figure 2. Mesh topology Network

Figure 2 shows the wireless random network. In this network, each node has a communication range which represents a distance, so any nodes falls in this range is considered a neighbor. As result of this, the gossip protocol will work between a node and its immediate neighbors.

Nodes which are in the communication range of that node, called immediate neighbors of the node. There is a one server node which is picked beforehand to maintains the security patch for this network

III. Failure models

We implemented two types of models the Byzantine General model and the wormhole attack failure model.

A. The Byzantine General failure model

Nodes in the network are aware of their surroundings, so nodes send and receive readings, exchange the newest version of temperature in the area. The nodes send each other the current temperature every time *t*. The way we implemented this failure model as it shown in Figure 1, node 9 is the Byzantine node that was changed by an outsider to behave in a smart way to mislead its neighbors. The number resembles the version of the reading.

A node requests for updates from its neighbors and compares its reading to them, if the neighbor has an older reading(less than 9), then it won't pass its new data to this neighbor for them, furthermore, it will deceive the neighbor and tell him that it has the same patch as them. Meanwhile, it tells the truth about its latest patch request if a neighbor has a newer version of the data. As result, this intruder is not of any use to the network. Node 9 will get a value of 10 from its neighbor so it will pass 9 to this node, and update its value with the latest patch. As a result this node will not benefit its other three neighbors who have very old versions of the data.

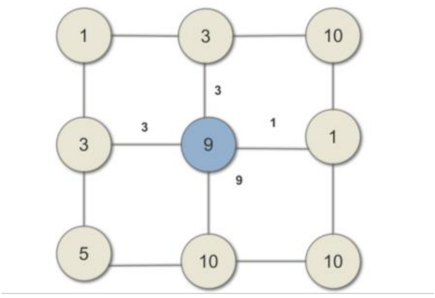

Figure 3. Byzantine node in a mesh topology

B. Wormhole failure model

The wormhole attack is a severe threat against packet routing in sensor networks that is particularly challenging to detect and prevent. In this attack, an adversary receives packets at one location in the network and tunnels them (possibly selectively) to another location in the network, where the packets are resent into the network[12]. An instance of a wormhole attack would involve two distant malicious nodes colluding to understate their distance from each other by relaying packets along an out-of-bound channel defined by the wormhole Start Point and the End Point available only to the attacker. Thus a false route would be established which would shorten the hop distance between any two non-malicious nodes.

Wormhole attacks can cause Denial-of-Service through Data Traffic, Denial-of-Service through Routing Disruptions and Unauthorized Access. In Denial-of-Service through Data Traffic, the malicious node(s) can insinuate itself in a route and then drop data packets. Denial-of-Service through Routing Disruptions can prevent discovery of legitimate routes and Unauthorized Access could allow access to wireless control system that are based on physical proximity, e.g. wireless car keys.

An intruder usually attracts network traffic by advertising

IV. Simulation

We have used Matlab simulation, to implement the failure models to the network. We deployed a small number of nodes *N* at first, such as *N*=200 then tried the same simulation after increasing *N* gradually up to 10,000 nodes. All nodes are placed on a 100 X 100 grid. We assign a node to play the role of server so that it keeps updating the network with the latest patch. Every random number of iterations it passes to the network a newer patch. And this patch propagates through the network. If the network stabilizes before this random time comes around then the simulation ends when all nodes are up to date.

In all simulations we started simple and then we increase the complexity of the network as time goes on, we start with 200 nodes up to 10000. Initially patches are randomly distributed to the network and randomness ensures that some nodes have updated patch. This leads propagation fast because every node gets higher version from its neighbors as well as up-to-date to server. We start with the latest patch =15 and increments after a random amount of time *t*.

Another changing parameter is the intruder size, we start off with only one intruder then we run the whole simulation and in another round we try to increase the number of intruders to see how long the network can tolerate these attacks.

- *Algorithm*
  - *For each node, do the following*
    - *Finds it neighbors*
    - *Check for each neighbor's patch*
    - *If it has higher patch, request and update your patch*
    - *Else push your patch to it*
    - *Repeat the process for each neighbors*
- *Repeat whole process for the network until every node has latest patch as server has.*

V. Analysis and Evaluation

Performance study has been stated following graphs for different parameter sets.

A. Performance study for general case

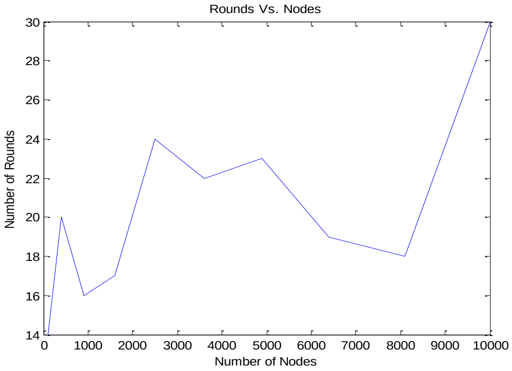

Figure 4. Network size Vs. number of iterations for mesh

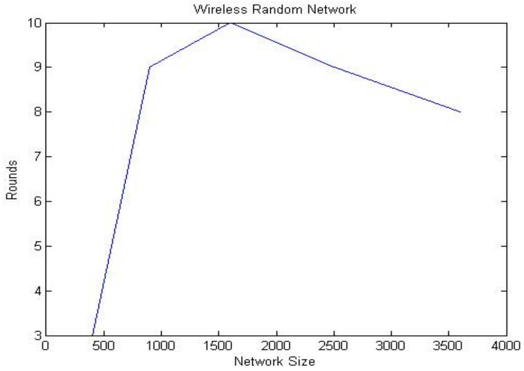

Figure 5. Network size and number of rounds for random deployment

In Figure 4 and Figure 5, show the relationship between the rounds(iterations) required to stabilize the network for different network size network. In mesh topology, the network can tolerate more intruders than random topology, because there is a big number of neighbors per node that results in making the network more sensitive to intrusion.

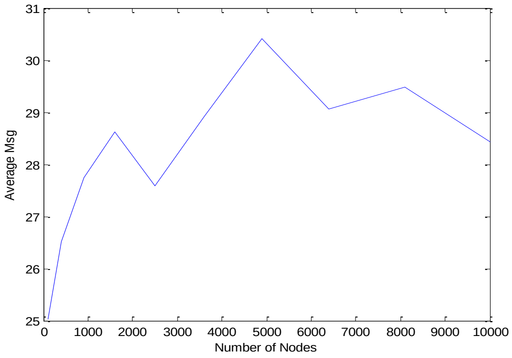

Figure 6. Network size Vs. number of rounds for mesh

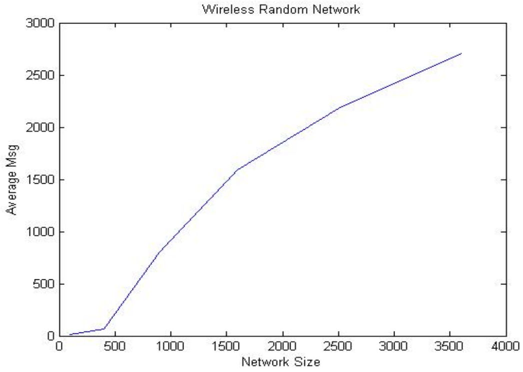

Figure 7. Network Size Vs. average number of messages exchanged for random network

In Figure 6 we tested the network size, as we increase the number of nodes, the average number of messages sent/received per node, it shows a big difference between the two, it is way bigger in the random network, due to the fact each node has a big number of neighbors more than mesh, so that adds up in each iterations more messages exchanged back and forth among neighbors comparing their patches, then number grows as we increase the network size.

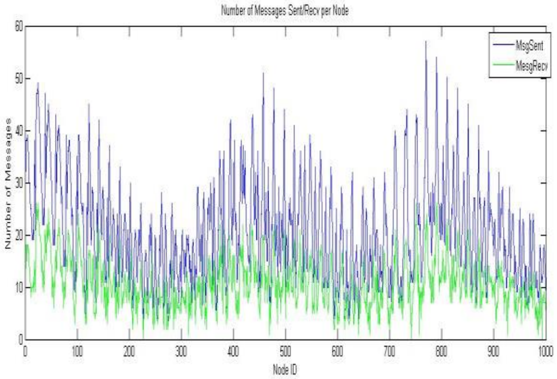

Figure 8. Number of messages sent/received vs. node id for Mesh Network

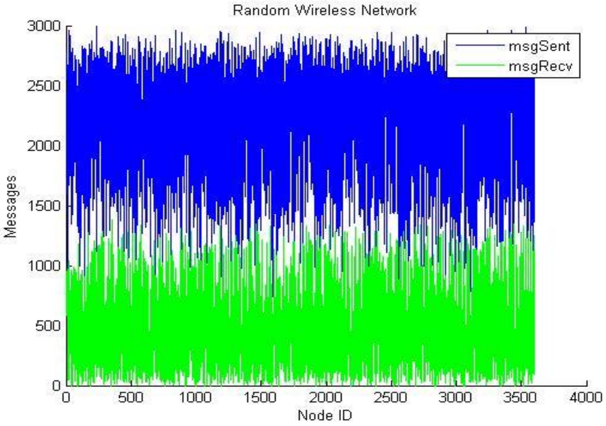

Figure 9. Number of messages sent/received vs. node Id for random network

Figure 8 and figure 9 show the total number of massages exchanged per node in the network; it is bigger for the random network for the same reason explained for figure 6 and 7.

B. *Performance Evaluation*

We have injected some nodes to the network that behave abnormally, in the sense that it does not harm other nodes but it does not benefit them so that will cause delay in having all nodes updated. While somebody pushes patch which is lower than its patch, it does not accept while it accepts the patches which are higher than its patch. This way network takes more time when number of failed nodes is higher. Following are the performance results for failure model.

1) Byzantine General failure model

We tested how long the network can survive a Byzantine attack, so increase the number of intruders (the Byzantine failure model explained before), and run the simulation to see how long the network can tolerate this intruder. what we are looking for is to have all the nodes are up to date.

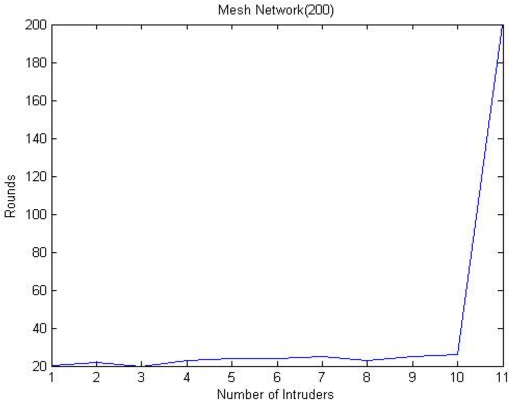

Figure 10 Number of intruder Vs rounds in a mesh network

In figure 10 we see that the network can survive up to 10 intruders, then the iteration number jumps to infinite number of iterations, then we know that we no longer can handle this kind of attack

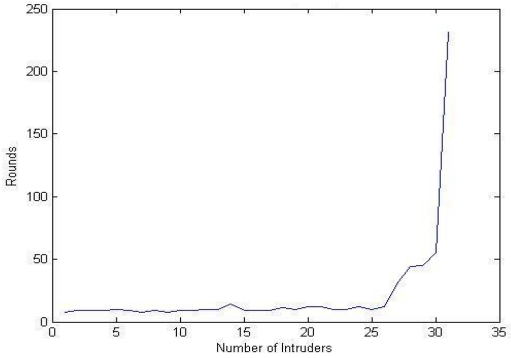

Figure 11. Number intruder vs. rounds in random network for 200 nodes

In random network it can tolerate up to 30 intruders when we have 30 infected nodes, whereas we can handle only 10 intruders in mesh network.

2) Wormhole failure model

We tested this attack by injecting one intruder into the network that behaves as sinkhole intruder, then increased the total number of nodes. And tested how long can the network survive. mesh network was able to handle only 4 intruders in the wormhole attack, versus it was able to handle 10 in the Byzantine attack.

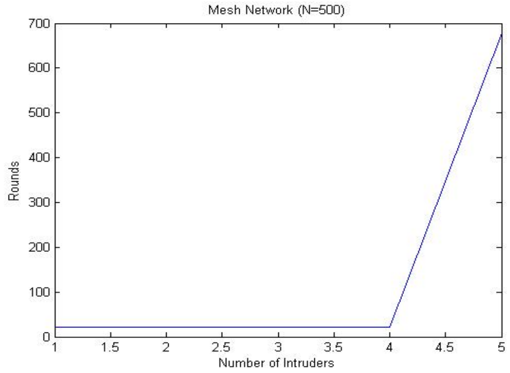

Figure 12. Number of intruders vs. rounds in mesh network

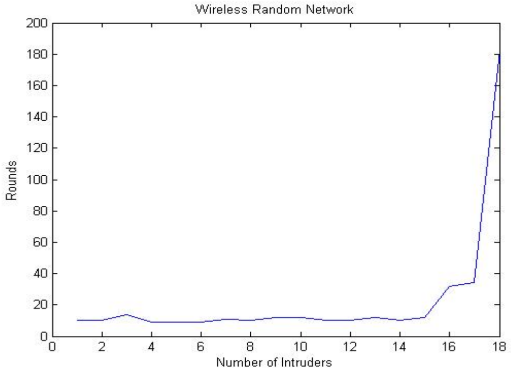

Figure 13. Number of intruders vs. rounds in random network

In figure 13 a random network of wormhole attack can handle up to 17 intruders versus in Byzantine attack it handled 30 for the same number of nodes in the network, so it can tolerate more intruders with this type of attack than Byzantine intruder.

VI. Conclusion

Different topologies of network can affect the overall tolerance of anytime of attack, in this paper, we tested two kinds of networks, mesh and random network. And we simulated two types of attack in these two, sinkhole attack which is one type of wormhole attack, and the Byzantine General failure model. We concluded that random network topology is more sensitive to attacks versus mesh topology due to the big number of nodes that will be infected by this intruder. We included also that a Byzantine General attack is more dangerous on the network, in terms of misleading its latest data from it neighbors

For future work, we would like to continue on our implementation of detecting the failed node using the Byzantine General fault tolerance model. As well as testing it on other topologies.

References

[1] R. A. F. Mini, B. Nath, and A. A. F. Loureiro, “A probabilistic approach to predict the energy consumption in wireless sensor network,” In IV Workshop ,” In IV Workshop on Wireless Communication and Mobile Computing, Seo Paulo, Brazil, October 23-25 2002.

[2] D. Dong, Y. Liu, X. Li, and X. Liao, “Topological detection on wormholes in wireless ad hoc and sensor networks,” IEEE Transactions on Networking, vol. 19, 2011.

[3] J. Kim, D. Sterne, R. Hardy, R. K. Thomas, and L. Tong, “Timing-based localization of in-band wormhole tunnels in manets,” in ACM WiSec, 2010.

[4] S. R. D. R. Maheshwari, J. Gao, “Detecting wormhole attacks in wireless networks using connectivity information,” in IEEE INFOCOMM, 2007.

[5] Y.-C. Hu, A. Perrig, and D. B. Johnson, “Wormhole attacks in wireless networks,” IEEE Journal on Selected Areas in Communications, vol. 24, no. 2, 2006.

[6] S. Dolev, “Gossiping in a multichannel radio network: An oblivious approach to malicious interference”., DISC, 2007.

[7] Amitanand , “BAR Fault Tolerance for Cooperative Services”, SOSP 2005.

[8] N. Alrajei, G. Corser, H Fu, Y. Zhu “Energy Prediction Based Intrusion Detection in Wireless Sensor Networks,” International Journal of Emerging Technology and Advanced Engineering (IJETAE, ISSN 2250–2459 Online, ISO 9001:2008 Certified Journal) Volume 4, Issue 3, March 2014.x

[9] N. Alrajei, H Fu, Y. Zhu "Information Theory based Intruder Detection in Sensor Networks", Journal of

[10] Communications Technology, Electronics and Computer Science, Volume 5, pp11-21, ISSN: 2457-905X, 2016

[11] N. Alrajei, H Fu, Y.Zhu “A Survey on Fault Tolerance in Wireless Sensor Networks” , 2014 American Society For Engineering Education North Central Section Conference ASEE NCS Conference April 4 and 5, 2014

[12] Yourong Xu et al, “Distributed Wormhole Attack Detection in Wireless Sensor Networks”, CIP 2007.