International Journal of Electronics Communication and Computer Engineering
Volume 5, Issue 6, ISSN (Online): 2249–071X, ISSN (Print): 2278–4209

Performance Evaluation of Black Hole Attack in Wireless Sensor Network

Manjunatha R C
Research scholar, Jain University
Bangalore, INDIA
email:lakshmikanth18@gmail.com

Rekha K R
Professor, Department of ECE
SJBIT, Bangalore
email:rekha.sjbit@gmail.com

Nataraj.K.R
Professor, Department of ECE
SJBIT, Bangalore
email:nataraj.sjbit@gmail.com

***Abstract*—Wireless sensor network are prone to various security threats. Increasing use of sensor networks necessitates that all security issues should be checked a priory. This paper focuses on creation of test scenario to evaluate the performance of sensor system under clone attack. Since clone attack is an insider attack, it may cause severe damage. Cooperative black hole attack is considered as a consequence of clone attack. Simulation scenario is created using MATLAB-2010a and network throughput is considered for performance evaluation.**

***Keywords*—Wireless Sensor Network; Clone Attack; Cooperative Black Hole Attack; Test Scenario.**

1. INTRODUCTION

Wireless sensor network is a collection of several tiny devices with limited memory, low computational capability and extremely limited energy supply [1]. These networks are usually deployed in hostile environments for their unattended nature [2], which makes nodes in the network dangerous to be captured by an adversary [3].There are many security threats to WSN, an attacker can snoop transmission, inoculate false data into the network, reroute the network transmission. To be secured a network must support confidentiality, integrity, authenticity and availability [4]. Node replication is a type of attack in which an attacker compromises the deployed nodes, extracts network keys with essential information and deploys replica nodes with same information but at some different location. These replica nodes act as part of network and therefore eligible to conduct any of inside attacks such as DoS attack, Sybil attack and Black hole attack [5]. This paper focuses on wireless sensor network threat model based on Node replication based black hole attack. The rest of this paper is arranged as follows: section II gives idea about security attacks in WSN, adopted sensor network and adversary model are described in section-III. Section-IV proposes clone based black hole attack model with experimental setup in section-V, result and discussion section-VI. Finally section-VII concludes this paper.

2. SECURITY ATTACKS IN WSN

Application area of wireless sensor network makes it susceptible to many attack, these attacks can be categorized as [7]

1. Layer wise: this type of attack can be further classified into five layers of operation of wireless networks i.e. physical layer, data link layer, network layer, transport layer and application layer based attacks. Frequency selection for transmission, carrier frequency generation, modulation, encryption and signal detection are the responsibilities of physical layer, while data link layer is responsible for medium access control, data stream multiplexing, data frame detection and error control. Routing and data delivery are done by network and transport layer respectively while application layer is responsible for applications communicating between hosts [2].
2. Type wise: these attack include network monitoring, close-in attacks, insider attacks including exploitation and service provider related attacks.
3. Passive attacks: passive attacker basically monitors unsecured traffic and try to steal the passwords and sensitive information of the network. This type of attacks include monitoring unencrypted communication, decrypting weakly encrypted data, traffic analysis and stealing authentication information. Passive intervention of network enables the attacker to judge the upcoming events and makes him able to apply the interruption.
4. Active attacks: in this type of attack, attacker actively tries to break security of network through viruses, worms or Trojan horses. These attacks include efforts to break network security in order to deploy malicious nodes.

Furthermore the attacks can also be categorized as:

Identity attacks, routing attacks and Network intrusion attacks. Identity attack tries to pilfer the identities of valid nodes working in the network. Sybil and clone (replication) attacks are identity based attack on wireless sensor networks. In Sybil attack, a malicious node owns multiple identities in order to subvert network performance while in clone attacks attacker creates multiple identities of a node and deploys them to different locations. In routing attacks, attacker attempt to interfere data transmission by placing malicious nodes in route from source to destination. Selective forwarding, sinkhole, wormhole and false routing are some of the routing attacks. In sinkhole attack, a large sphere of influence is created by the adversary which attracts all the traffic destined for base station towards them. False routing attack includes injecting fake control packets in the network. Forwarding selected packets or discarding selected portion of data is part of selective forwarding attack. Nomenclature of security attacks on WSN is given in figure-1[6]:

International Journal of Electronics Communication and Computer Engineering
Volume 5, Issue 6, ISSN (Online): 2249–071X, ISSN (Print): 2278–4209

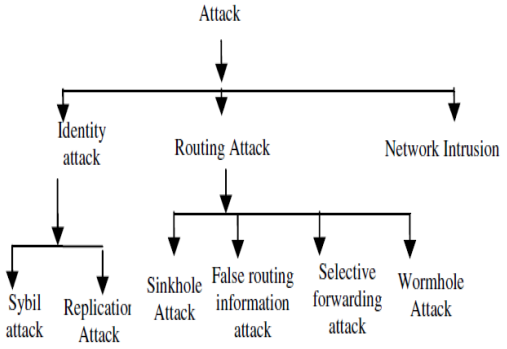

Figure-1: Security attacks on Wireless Sensor Network [6]

3. Sensor Network Environments and Adversory

A wireless sensor network may comprise of several hundreds of tiny low cost devices known as sensor nodes which are randomly distributed over a field for monitoring. Wireless sensor networks are scalable in nature i.e. nodes may be added or removed during run time.Base station is the centralized authority which is responsible for data collection and network monitoring related tasks. Many applications avoid a centralized fixed point of failure, in such cases distributed sensor network is required where data collection is carried out by mobile units. In our threat model, network is suppose to be centralize, where base station handles all network related reposibilities. Sensor nodes are loaded with predifiend public and private key pair generated by RSA key generator[9,10]. It is supposed that data transmission occures at irregular intervals and attacker has enough time to perform clone attack.Once replica nodes are deployed attacker can corrupt data, retire authentic nodes or destabilise network operation. It is also assumed that an adversary can only capture a fraction of node while it is not capable of creating new IDs.[8]. While exploring threat model to wireless sensor networks, a conventional approach is assumed where an adversary can only corrupt a limited number of nodes. Let K be the percentage of total nodes that can be influenced by the attacker(less than 20%). By limiting the percentage of nodes we are avoiding the probablity of network brakdown as we are only intersted in evaluating the impact of attack on the performace of system. It is also assumed that adversary uses unshielded nature of sensor nodes to steal their cryptographic information. The adversary than fed some generic sensor nodes with this information and deploys them in the field. We have restricted the number of clone of any legitimate node to 1, also mobile data collection points are considered for performance evaluation. Attacker is assumed to apply black hole attack through clone nodes.

4.Proposed Approach

This paper is focus on creating a test scenario for wireless sensor network using clone based cooperative black hole attack. Clone attack is an identity based attack in which an adversary node steal the authentication information of legitimate node and uses this information to deploy generic nodes in the field. Figure-2 shows basic clone attack in wsn.

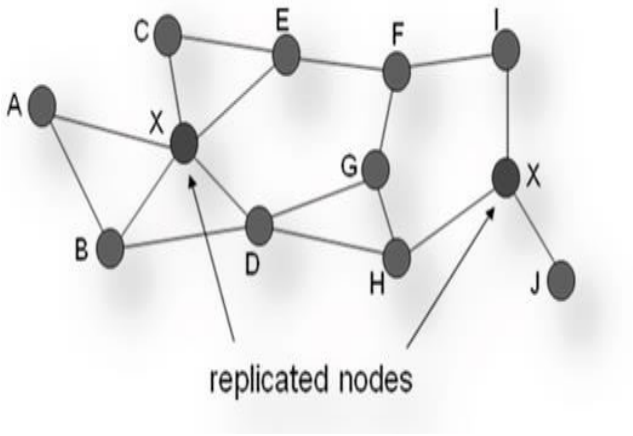

Figure-2: Clone attack [6]

The severety of clone attack can be estimated from the figure above, node-X is part of network which is replicated at some other position also. Since the attacker is successful in placing the node inside the network, it can apply several attack also. We have considerd cooperative black hole attack as a consequence of clone attack.

Black hole attack[11] is a type of internal attack on sensor network in which malicious node fits between the route of source and destination. As soon as this malicious node gets chance, this malicious node make itself active data route element. Now it is capable of conducting attacks with the start of data transmission.

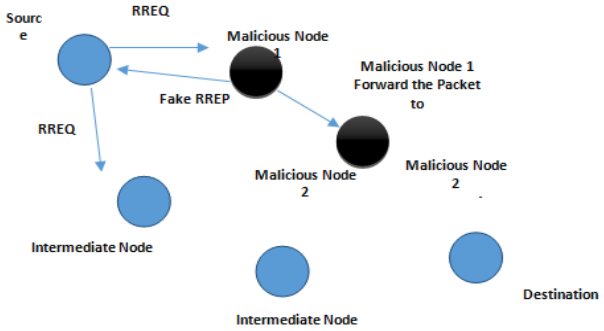

Figure-3: Black hole attack [11]

A Clone based cooperative black hole attack:

In our test scenario network with 100 nodes is considered. These nodes are uniformly distributed over an area of 100×100 square meters. Each node is loaded with a unique public and private key pair generated by RSA algorithm. Base station occupies the database of member nodes with theire authentication information. In out test model attacker tragerts node within a specified range from the base station. If the targated device lies within the specified range its clone will be created at some other place within the network with the same identity information and with infinite energy resource. These clone nodes will fit in the network and be a part of network

operation. As soon as this nodes gets chance they will start conducting cooperative black hole attack. A mobile attacker is considered to which these malicious nodes reroute the network transmission.

At the start of every round, public and provate key pair is firstly checked with the data saved at base station, the authorize nodes only get a chance to operate network task based on LEACH clustering algorithm. Since the clone nodes have the cryptographic information they were assumed to be able of penetrating network security

.

TABLE 1: SIMULATION PARAMETERS

Network Operation	**Energy Dissipation**
Transmitter/Receiver Electronics	$E_{elect} = 50nJ/bit$
Data Aggregation	$E_{DA} = 5nJ/bit/report$
Transmit Amplifier if $d_{toBS} \leq d0$	$\epsilon_{fs} = 10pJ/bit/m2$
Transmit Amplifier if $d_{toBS} \geq d0$	$\epsilon_{mp} = 0.0013pJ/bit/m4$

5. EXPERIMENTAL SETUP

For simulation purpose an area of 100x100 meters squares is considered with 100 nodes uniformly distributed over the field. RSA based public and private key generator is used, each node in the network is preloaded with unique public and private key pair. Base station is centralized controlling authority which saves node related information. Simulation parameters and standard energy consumption values are given in table-2 and table-3 respectively. Network lifetime, Network throughput are chosen as parameters for performance evaluation. MATLAB-2010a is simulation tool for our research.

TABLE 2: ENERGY DISSIPATION OF WIRELESS SENSOR NETWORKS

Field Dimension	100x100
Number of Nodes	100
Election Probability	0.1
Percentage of heterogeneity	0.1, 0.2
Alpha	2, 3
Number of Rounds	2000
Number of clones allowed	< 2%

6. RESULTS AND DISCUSSION

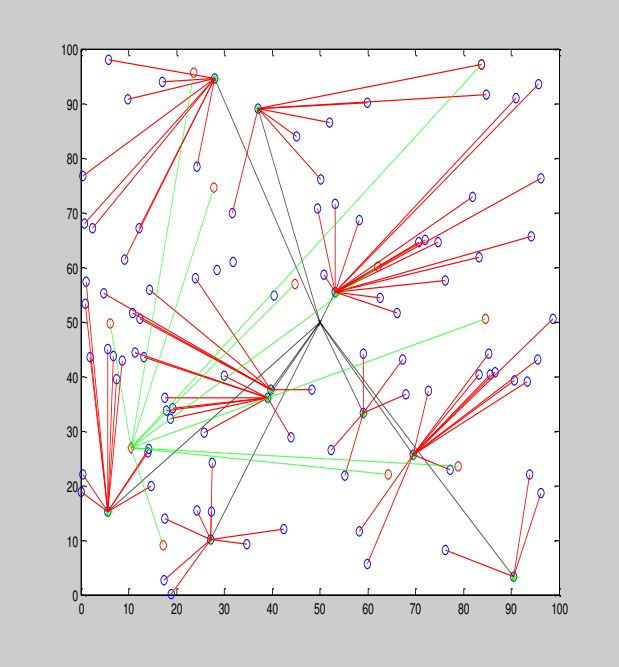

Figure-4: Simulation of Clone based Black-hole Attack model (Black lines: Data to BS, Green lines: Data to attacker at position-1)

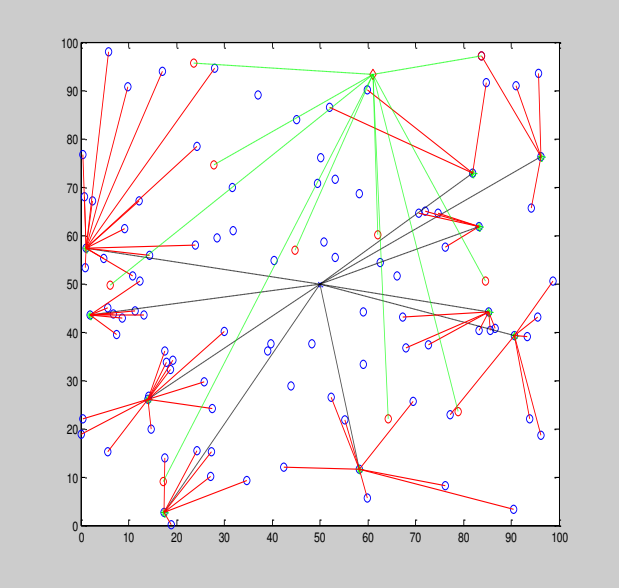

Figure-5: Simulation of Clone based Black-hole Attack model (Black lines: Data to BS, Green lines: Data to attacker at position-2)

Simulation of our proposed test scenario is depicted in figures-4, 5. Blue circles being legitimate nodes, red ones being their clone. It can be observed form the figures that legitimate nodes report to central base station while clone node reroute the transmission towards the mobile attacker (black and green dashed lines in the figure respectively).

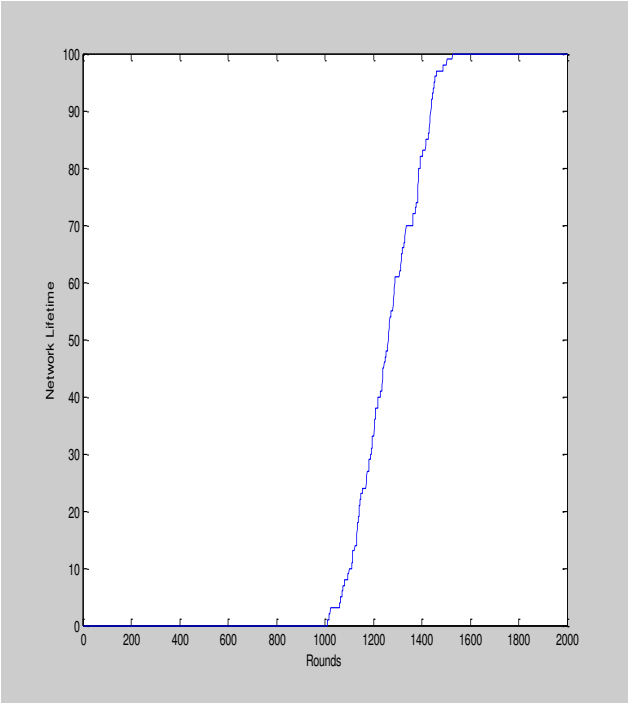

Figure-6: Lifetime of devices under Clone based black hole attack

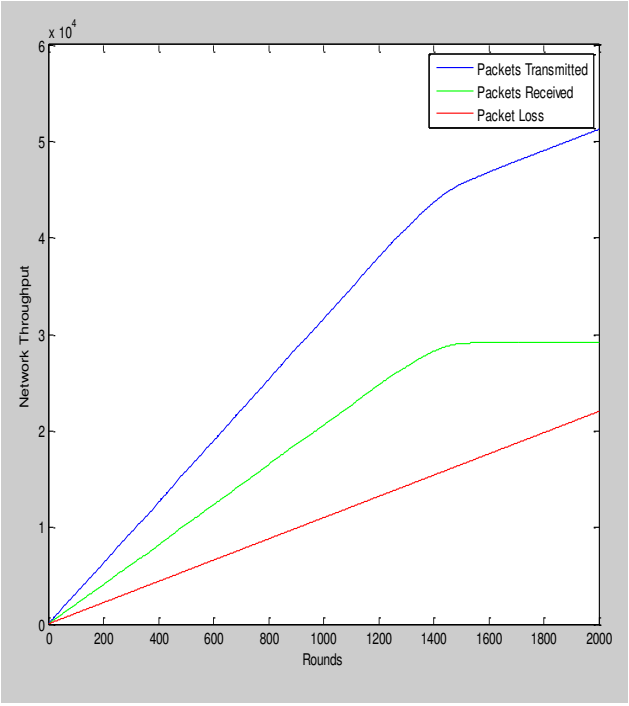

Figure-7: Variation of network throughput under clone based black hole attack (Packets transmitted, Packets received and packet loss)

Lifetime of devices and network throughput under given test scenario is given in figures-6&7respectively. The proposed test scenario does not affect lifetime of devices while its impact can be directly observed on throughput of the network. Table-3 gives information about the loss of network throughput.

TABLE 3: IMPACT OF CLONE BASED COOPERATIVE BLACK HOLE ATTACK ON NETWORK THROUGHPUT

Total Number of packets transmitted	Number of packets received at BS	Number of packets to attacker	Throughput Loss
51227	29216	22011	42.96%

7. CONCLUSION

Test scenario to evaluate the performance of wireless sensor network under clone based cooperative black hole attack is simulated in this paper. MATLAB based model for RSA key generator and wireless sensor network is considered. Mobile adversary with ability to capture 20% of total nodes is considered for performance evaluation. Impact of clone based cooperative black hole attack is revealed through the loss of network throughput. Simulation results shows that approx. 42% of total packets were lost during network operation.

REFERENCES

[1] TmoteSky wireless sensor module. http://www.moteiv.com/products/docs/tmotesky-datasheet.pdf
[2] Akyildiz, Ian F., et al. "Wireless sensor networks: a survey." *Computer networks* 38.4 (2002): 393-422.
[3] Karlof, Chris, and David Wagner. "Secure routing in wireless sensor networks: Attacks and countermeasures." *Ad hoc networks* 1.2 (2003): 293-315.
[4] Perrig, Adrian, et al. "SPINS: Security protocols for sensor networks." *Wireless networks* 8.5 (2002): 521-534.
[5] Parno, Bryan, Adrian Perrig, and Virgil Gligor. "Distributed detection of node replication attacks in sensor networks." *Security and Privacy, 2005 IEEE Symposium on*. IEEE, 2005.
[6] Manjula, V., and C. Chellappan. "The replication attack in wireless sensor networks: analysis and defenses." Advances in Networks and Communications. Springer Berlin Heidelberg, 2011. 169-178.
[7] Gupta, Sunil, Harsh Kumar Verma, and A. L. Sangal. "Authentication protocol for wireless sensor networks." *Paper at World Academy of Science, Engineering and Technology* (2010).
[8] Newsome, James, et al. "The sybil attack in sensor networks: analysis & defenses." Proceedings of the 3rd international symposium on Information processing in sensor networks. ACM, 2004.
[9] H. Chan, A. Perrig, and D. Song. Random key predistributionschemes for sensor networks. In Proceedings ofIEEE Symposium on Security and Privacy, May 2003.
[10] L. Eschenauer and V. Gligor. A key-managementscheme for distributed sensor networks. In Proceedings of the ACM Conference on Computer and Communication Security (CCS), Nov. 2002.
[11] Al-Shurman, Mohammad, Seong-Moo Yoo, and Seungjin Park. "Black hole attack in mobile ad hoc networks." *Proceedings of the 42nd annual Southeast regional conference*. ACM, 2004.

AUTHORS PROFILE

Manjunatha R Cobtained his B.E and M.Tech Degree from Visveshwaraya University, Karnataka, India, in 2006 and 2008 respectively in Telecommunication Engineering. He is working as Assistant professor at Acharya Institute of

Technology, Bangalore, and Karnataka. He is currently pursuing his Ph.D at Jain University, Karnataka. His current research includes Clone detection in wireless Sensor Networks.

Dr K. R. Rekha obtained her ME degree from Bangalore University, India in 2000. She is working as a Professor in the Department of Electronics and Communication in SJB Institute of Technology, Bangalore. she has pursued her Ph. D. degree in Dr MGR University, Chennai. Her research interests include Wireless communication, FPGA implementation, and Microcontroller and Embedded systems design. She is a member of MIE, MISTE and IETE

Dr K. R. Nataraj obtained his ME degree from Bangalore University, India in 2000. He worked as Professor and Head of the Department during 2000-2008 and currently he is the Post Graduate Coordinator in the Department of Electronics and Communication in SJB Institute of Technology, Bangalore. Presently, His research interests include Wireless communication, FPGA implementation, and Microcontroller and Embedded systems design. He is a member of MIE, MISTE , IETE and IEEE