International Journal of Applied Engineering Research
ISSN 0973-4562 Volume 10, Number 10 (2015) pp. 25929-25937

http://www.ripublication.com

A Novel Scheme For Detection of Selective Forwarding Attack and Sybil Attack In Wireless Sensor Network

Preeti Aggarwal, Dr.Mritunjay Kumar Rai
School of Electronics and Communication and Engineering
Lovely Professional University, Phagwara
{aggarwal.preeti6@gmail.com, raimritunjay@gmail.com }

Abstract

Wireless sensor network has become very popular in the research area because of its many out-door applications like military surveillance and civilian. But because of the wireless transmission media and limited resources, WSNs are very easily prone to security attacks specially Denial of service. The selective forwarding attack and Sybil attack are very popular attack on WSN. It is very difficult to detect these attacks. For detection of these attacks this paper suggests a novel scheme. The proposed technique is based on the network and local key to detect the selective forwarding attack and Sybil attack. To test the effectiveness of this method we have analyzed this method through NS2.35 simulator. Malicious nodes are efficiently detected and subsequently these nodes are eliminated from data propagation path. The performance of this method has been analysed in terms of energy consumption, delay and throughput.

Keywords: Wireless Sensor Network, Security, Selective Forwarding attack and Sybil attack.

Introduction

A Wireless Sensor Network is a group of independent nodes, which communicates in wireless medium. They have some special characteristics like low power utilization, constrained processing power and minute radio range. They provide low price solutions to various applications such as scientific examination, collection of data and monitoring and military applications. They require a high caliber of security because they are utilized in some serious applications such as medical and military applications. Sensitive data is create by the sensor network must be bulwarked against unauthorized access or from attacker to prevent the unwanted changes.

Wood and Stankovic gave a suitable definition of DoS attack, “any event that diminishes or eliminates a network’s capacity to perform its expected function”[1].

Most commonly DoS attacks are selective forwarding attack, Sybil attack, flooding attack, sink hole attack etc. In this paper we have discussed a novel technique to detect the selective forwarding attack and Sybil attack.

In selective forwarding attack the attacker nodes may refuse to forward some sensitive packets and simply drops them. Selective forwarding attack is type of black hole attack. Selective forwarding is most effective when this attack is explicit on data flow path. In a Sybil attack, multiple identities are presented by a single node to other nodes in a network. The effectiveness of fault tolerance is reduced by Sybil attack. Sybil attack can mislead the neighbor nodes in location based routing techniques.

Related Work

Karlof et al. [2] have discussed the selective forwarding attack first time and suggest a method to detect these types of attack by multi path routing. Here the message is transferred from different paths whose nodes are disjoint with each other and not involved the compromised nodes. The drawback of this method is large energy is consumed if more paths are formed.

Yu, B. and Xiao, B. [3] have proposed a scheme to detect the selective forwarding attack in network by using multi hop acknowledgments from intermediate nodes in the network. In this scheme detection takes place in base station as well as source node. In this paper author use the directed diffusion routing protocol. The main drawback of this scheme is lack of efficiency. Here to detect the selective forwarding attack sensor nodes make every effort.

Xiao, B. et al [4] have proposed a technique to detect the attacker node in selective forwarding attack. It is called as checkpoint based multi hop acknowledgment scheme (CHEMAS). In this technique author randomly pick some intermediate nodes which are present in forwarding path and select them as checkpoint nodes which generate the acknowledgments for every packet they received. Disadvantage of this scheme is to store the one way hash key to every node memory is used.

Hai, T. H. et al [5] have proposed a centralized based scheme. This technique is cluster based lightweight detection technique. In this technique the information required is of only two hop neighbor nodes. In this technique the sensor node activate the detection element which is known as monitor node and also has information of two hop neighbor. Drawback of this technique is if monitoring node is itself a compromised node there is no way to detect this.

Vamsi, P.R. et al [7] have proposed a sequential hypothesis method to detect the Sybil attack. A greedy perimeter stateless routing method is used to examine this scheme. In this scheme every node is participated. All the observations are carried by each node. The Sybil attack is detected by this method without having false impact of false positives and false negatives.

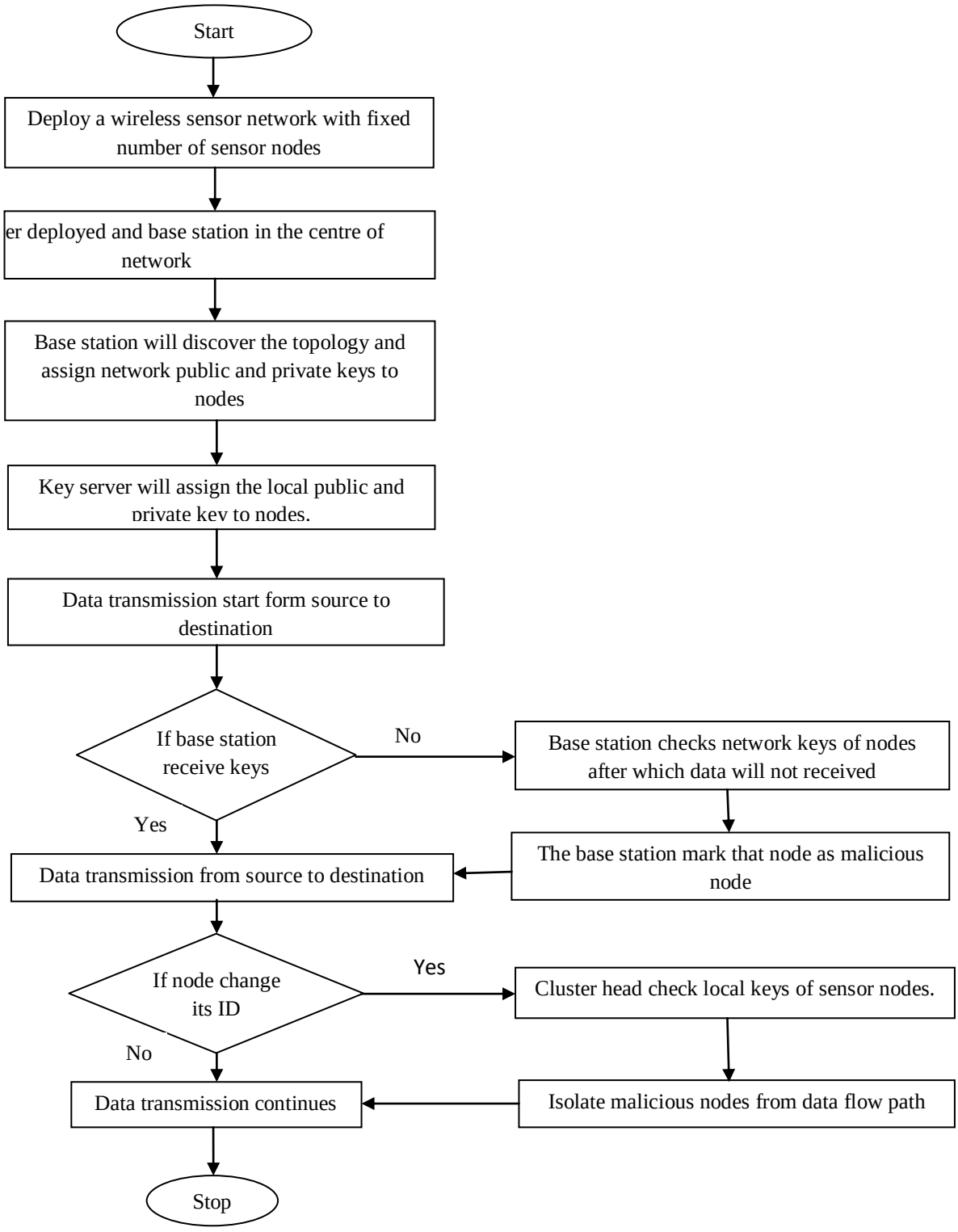
Triki, B. et al [8] have proposed a system to detect the Sybil attack in military wireless sensor network. Two type of authentication techniques are used to identification of Sybil attacker. In this method the leader of groups of solider is able to detect the Sybil nodes. By changing the identity of moving soldiers prevents from tracking by attacker. Privacy is also prevented by this method.

Problem Statement

The wireless sensor is the type of network which is used to sense environmental conditions like temperature, pressure etc. The sensor network is the self configuring and decentralized type of network due to which some malicious nodes may exits which is responsible to trigger certain type of security attacks which degrades network performance. In this work, selective packet drop and Sybil attack has been triggered by the malicious node in the network which will increase network energy consumption, reduce throughput and increase delay. The novel technique has been proposed in this work, to detect and isolate malicious nodes from the network which is responsible to trigger attack. The proposed technique will be based on network public and private key to isolate selective packet drop attack and local public and private key is used to isolate Sybil attack from the network.

Proposed Technique

In this work, technique has been proposed to isolate malicious nodes from the network which are responsible to trigger selective packet drop and Sybil attack in wireless sensor networks. In the proposed technique base station will discover topology of the network means information of every node their node id, location. After discovering topology of the network, base station will assign public and private key network keys to every node in the network. The whole network will be divided into four parts. The key server in the network will be responsible to assign local public and private keys to sensor nodes. The sensor nodes will start sending data to sink node. The malicious nodes which are responsible to trigger attack will drop data and sink will not receive that data. The sink will detect node as the malicious node after that node no data will be received. The base station will assume that all the detected nodes are malicious and these nodes are also responsible to trigger Sybil attack. The nodes will start sending data to its cluster head, if some node is changing its identification will be detected by the cluster head and cluster head pass that information to base station. The base station then finalizes that which are malicious and which are legitimate node on the bases of collected information.



Simulation and Results

Our aim is to recognize the attacker nodes that perform the selective forwarding attack and Sybil attack in the network. The simulation is implemented in NS 2.35, a

simulator for mobile adhoc network. The simulation parameters are given in Table I. The simulation time is 100.

Table 1: Simulation Parameters

Name	**Simulation parameters**
Routing protocol	AODV
Simulation area	1500*1150
Channel type	Wireless
Simulation time	100
Number of nodes	81
Attacker nodes	10
Mac Type	Mac/802_11

Results

In this section we analyze the simulation results are mentioned with the scenario of during selective forwarding attack and Sybil attack and with proposed technique.

1. Energy consumption: The energy consumption of the filed during attack and after the detection of malicious nodes.

Table 1: Comparison of Energy Consumption During Attack and After Detection

Time (in s)	**Energy consumption during attack (joules)**	**Energy consumption after detection of attack (joules)**
0	0	0
20	1.399	1.100
40	1.0588	1.0147
60	1.02924	1.0060
80	1.01646	1.0041

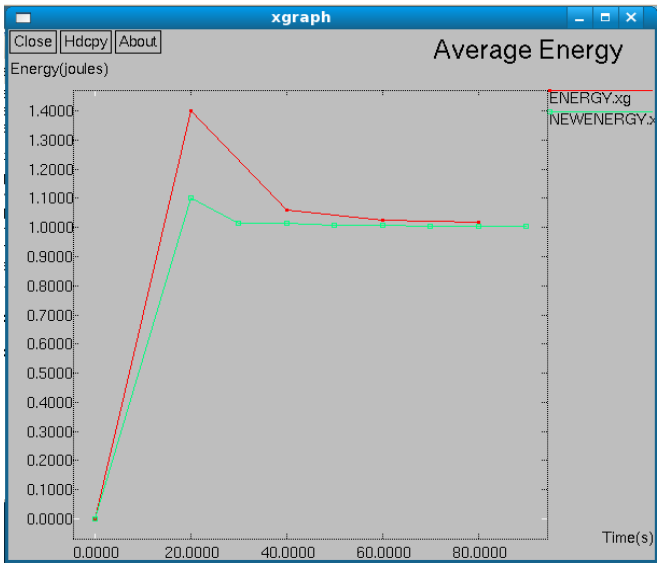


Figure 1: Energy consumption for Table I

2. Throughput: Number of packets sends per unit time. After detection of attack throughput is increased of network.

Table 2: Comparison of Throughput During and After Detection

Time (ins)	**Throughput during attack (Kb/s)**	**Throughput after detection of attack (Kb/s)**
0	0	0
20	0.02	0.032
40	0.136	0.2175
60	0.33	0.528
80	0.4859	0.7775

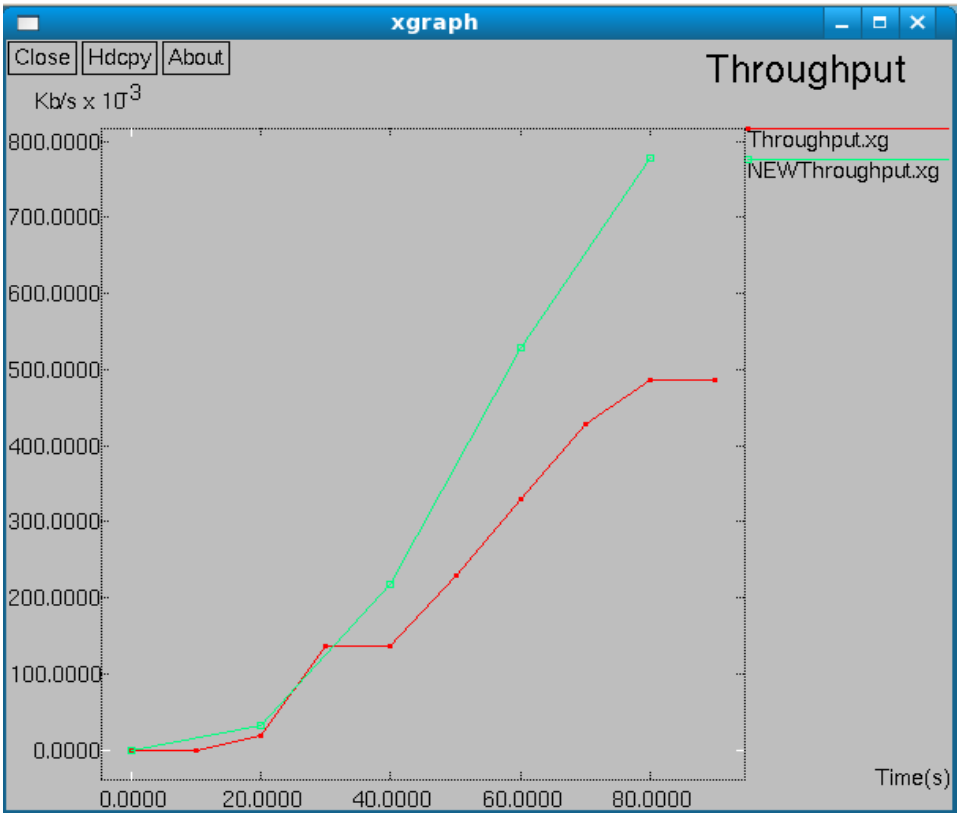


Figure 2: Throughput analysis for Table II

3. Delay: It is the total time taken for the packet to reach from source to destination and it is measured in seconds.

Table 3: Comparison of Delay during Attack and After Detection

Time (in s)	**Delay during attack (in s)**	**Delay after the detection of attack (in s)**
25	0.0001	0.0001
45	0.0012	0.0010
65	0.0025	0.0021
85	0.0049	0.0039
95	0.0051	0.0041

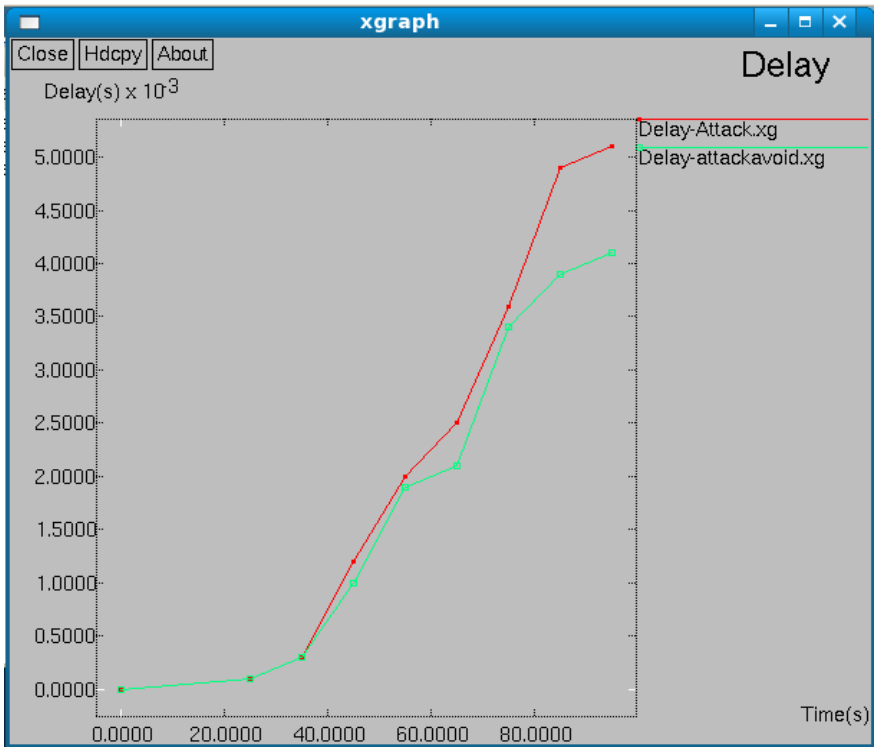


Figure 3: Delay analysis for Table III

Conclusion

The sensor network is the self configuring and decentralized type of network due to which some malicious nodes may exits which is responsible to trigger certain type of security attacks which degrades network performance. In this work, selective packet drop and Sybil attack has been triggered by the malicious node in the network which will increase network energy consumption, reduce throughput and increase delay. The novel technique has been proposed in this work, to detect and isolate malicious nodes from the network which is responsible to trigger attack. The result of our implementation show better impact to overcome selective forwarding attack and Sybil attack. This technique significantly improves system performance and we find that the method introduced is efficient because it detect selective forwarding and Sybil attack with less delay, less energy spent, more throughput.

References

[1] Wood, A. D. and Stankovic, J.A. (2002) "Denial of Service in sensor networks", Computer, vol.35, no.10, pp.54-62.

[2] Karlof, C. and Wagner, D. (2003) "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures", proceeding in IEEE, Vol. 1, No. 2, pp.113-127.

[3] Yu, B. and Xiao, B. (2006), "Detecting selective forwarding attacks in wireless sensor networks", in Proc. of the 2nd International Workshop on Security in Systems and Networks, IEEE, pp. 1-8.

[4] Xiao, B., Yu, B. and Gao, C. (2007), "CHEMAS: identify suspect nodes in selective forwarding attacks," in Journal of Parallel and Distributed Computing, Vol. 67, No. 11, pp. 1218-1230.

[5] Hai, T. H. and Huh, E.N. (2008) "Detecting Selective Forwarding Attacks in Wireless Sensor Networks Using Two-hops Neighbor Knowledge", in proceedings of Seventh IEEE International Symposium on Network Computing and Applications, pp.325-331.

[6] Deng, H., Sun, X., Wang, B. and Cao, Y. (2009), "Selective Forwarding Attack Detection using Watermark in WSNs", International Colloquium on Computing, Communication, Control, and Management (ISECS), pp.109-113.

[7] Vamsi, P.R. and Kant, K. (2014), "Sybil Attack Detection using Sequential Hypothesis Testing in Wireless Sensor Networks", International Conference on Signal Propagation and Computer Technology (ICSPCT), pp. 698-702.

[8] Triki, B., Rekhis, S. and Boudriga, N. (2014), "An RFID based System for the detection of Sybil attack in Military Wireless Sensor networks", IEEE.

[9] Makhdoom, I., Afzal, M. and Rashid, I. (2014), "A Novel Code Attestation Scheme Against Sybil Attack in Wireless Sensor Networks", National Software Engineering Conference, pp. 1-6.