Hindawi Publishing Corporation
ISRN Sensor Networks
Volume 2013, Article ID 843626, 9 pages
http://dx.doi.org/10.1155/2013/843626

Research Article

Detection and Countermeasure of Node Misbehaviour in Clustered Wireless Sensor Network

Meenakshi Tripathi, M. S. Gaur, V. Laxmi, and P. Sharma

Malaviya National Institute of Technology, Jaipur 302017, India

Correspondence should be addressed to Meenakshi Tripathi; tripathimeenu@yahoo.co.in

Received 15 August 2013; Accepted 18 September 2013

Academic Editors: J. Li and Y.-C. Wang

Wireless sensor networks are widely used in many applications like battlefield monitoring, environment monitoring, and so forth. In all of these applications the cooperation among various sensor nodes is needed to forward the data packets to the base station. However, it expends the various resources of a sensor node such as battery power, storage, and processing power. Therefore, to conserve its own resources a node may become selfish by not forwarding the data to the others. This kind of attack has serious consequences if the attacker node is the leader of a cluster. In the presence of attack the base station will not be able to get the data from the victimized cluster while resources of the member of that cluster are being consumed. In this paper we propose a scheme called *window based scheme (WBS)* to detect this kind of misbehavior in WSN. Our detection scheme is energy efficient because most of the computations are done at base station only. Simulation results prove that our method detects and removes the attacker effectively and efficiently.

1. Introduction

A wireless sensor network (WSN) [1] is a self-organizing network consisting of hundreds to thousands of sensor nodes. Each sensor node has limited processing, storage, and computational capability. A sensor node "senses" various parameters like humidity, temperature, pressure, motion, vibration, and so forth, according to the requirement of WSN application, converts it into appropriate signal, and forwards it to a central authority known as a base station or sink through the wireless medium. Base station may again send it to another base station or can take the decision based on acquired data on its own.

These networks are widely used in various applications like battlefield surveillance [2], environmental monitoring [3], wildlife monitoring [4], and so forth. In most of the applications the WSN is set up in a hostile environment in an ad hoc manner, which makes them vulnerable to several types of security threats [5]. To enhance the survivability of WSN, traditional security mechanisms like encryption, access control, and authentication have been used by the researchers. However, due to resource limitations strong security mechanism cannot be added to prevent misbehavior of a sensor node. These reasons will lead to abnormal functioning of the network.

Now a node may misbehave in various ways such as it does not forward the data at all (blackhole attack) or it may forward the data selectively or it may go into the sleep mode (snooze attack). The attacker may do it either due to any commercial benefit or to preserve its own resources. This behavior of the attacker will affect the data reached at the base station and can affect the overall decision taken by the user on the basis of the collected data. Another impact of this kind of attack is wastage of resources of all the cluster members of the victimized cluster. They are dissipating their energy in sensing as well as in communicating the signal to the head but ultimately their data is not able to reach the decision center.

In this paper we have proposed a method to detect the abovementioned attacks. Our work has three main contributions. First we explored the impact of node misbehavior in WSN. We have simulated various types of node misbehavior in wireless sensor network. Second, we have developed

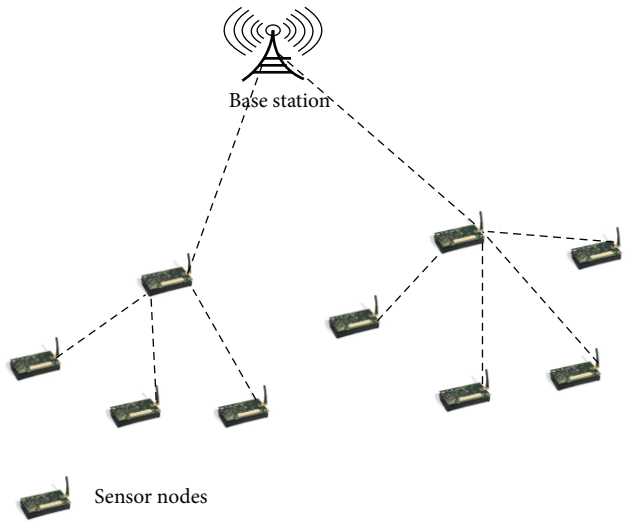

Figure 1: Wireless sensor network.

a scheme that detects the node misbehavior. Our scheme does not put any extra overhead on sensor nodes as most of the processing is done at base station only, which is a highly resourceful node. Finally we manifest the effectiveness of our scheme by simulating various node misbehavior methods in WSN. With our scheme we have not only identified the attacker but also removed it from the network, with very low false positive rate in various attacked scenarios.

Our paper is organized as follows. Section 2 gives an overview of WSN, its routing protocols, and security threats. Work done for the security of LEACH-C is described in Section 3. The attack modeling is discussed in Sections 4 and 5 gives the details of the proposed detection scheme. The simulation results are given in Section 6, and finally Section 7 concludes the paper.

2. Wireless Sensor Network

Wireless sensor network consists of spatially distributed autonomous sensors to monitor physical phenomena such as temperature, sound, and pressure. WSN provides a bridge to cover the gap between the physical and virtual worlds and allows the ability to observe the physical phenomenon at a fine resolution over large spatiotemporal scales. The sensor has a transducer that converts physical events into electricity or other signals that can be read by an observer or by a device. Sensor nodes are known as motes and super nodes are known as Base Station or Sink. We have shown in Figure 1 the basic architecture of a wireless sensor network.

In wireless sensor network sensor nodes are linked together to form a wireless network. All the sensor node communication happens in the air so a WSN faces all the problems of any other wireless network. Apart from this, some unique characteristics also pose new technical challenges for these networks. Some of those challenges are as follows.

(i) Limited resources: to have a long life of the network consisting of sensor nodes with limited memory, battery, and processing power, it is always advisable to implement the techniques to reduce both computation and communication cost.

(ii) Unattended operation: most of the time WSNs are deployed in hostile environment where it is difficult to make any changes after initial deployment.

(iii) Data-centric routing: emphasis is given on routing decisions which are based on the data possessed by the sensor nodes instead of the address.

(iv) No fixed topology: the number of nodes in the network keeps changing as the node may move out of the network either due to mobility or due to the drained battery.

All these challenges provoke the development of different kind of routing protocols for WSN. In the next section we will describe some of the routing protocols used by several researchers for WSN.

2.1. Routing Protocols for WSN. In WSN all the sensor nodes have to forward their data to the base station. This can be done either using *flat routing* or *cluster-based routing*. In flat routing protocols all the nodes are having the same functionality while in case of cluster-based routing some nodes have to perform some special tasks like aggregation or fusion on the data collected from several nodes. Flooding [6], rumor routing [7], and directed diffusion [8] are some of the flat routing protocols used in sensor networks. Cluster-based routing protocols are efficient in terms of energy consumption and network lifetime as compared to flat routing [9]. In these routing protocols a group of nodes form a cluster and all the nodes of a cluster have to send the data to their head only. Afterwards it is the responsibility of the head to compress the data and forward it either to the base station or to another cluster head. LEACH [10], TEEN [11], PEGASIS [12], and LEACH-C [13] are examples of cluster-based routing protocols for WSN.

In our research we have mainly concentrated on LEACH-C protocol which is a simple and efficient clustered protocol for WSN. In it the rotation of cluster head is done in an adaptive manner and the sensor nodes need not consume their energy in cluster formation; hence it outperforms other classical clustering algorithms in terms of energy distribution among various nodes. It is important to note that the fundamental of our scheme is not limited to LEACH-C; it can be used in any other hierarchical clustering algorithm. Now we explain the basic operation of LEACH-C.

2.2. LEACH-C. LEACH-C is an enhanced version of low energy adaptive clustering hierarchy (LEACH) protocol. In this protocol the clusters are formed by the BS. Each node sends its own location and residual energy to the BS at the start of every round as shown in Figure 2. Now base station runs a simulated annealing algorithm [14] to form the cluster head and their cluster members.

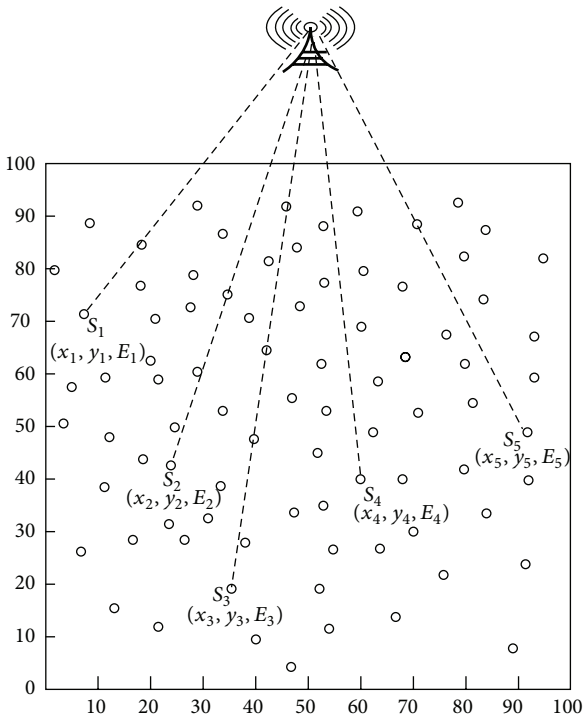

Figure 2: Location and current energy transfer to the BS.

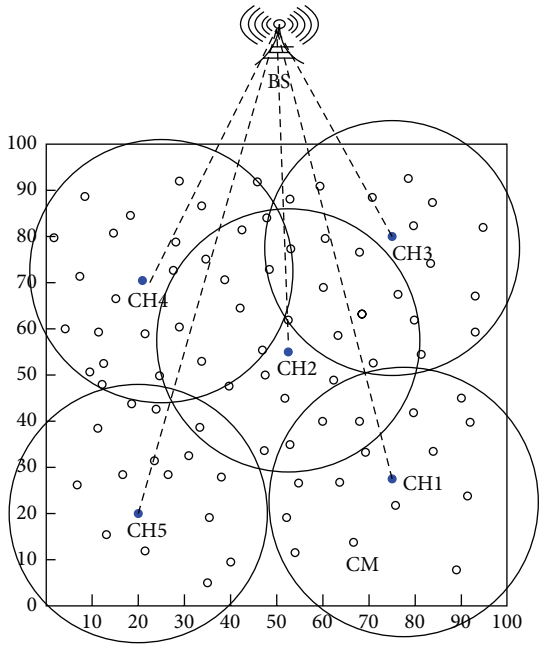

Figure 3: A WSN after cluster formation.

Base station broadcasts this cluster information to the network. All the nodes will check their IDs in this broadcasted information to find out whether they are a cluster head or a cluster member.

Once the clusters are formed the member will send their sensed data to the head in allotted time slot of a TDMA frame and after collecting the data from all the members for round time t_{round}, the cluster head will send aggregated data to the base station. In Figure 3 various CH (cluster heads) are transmitting data to the base station.

Initially all the nodes are eligible to become a cluster head. But later on the eligible cluster heads will only be those nodes whose energy is above the average energy of the network. This leads to the somewhat even distribution of load among all the nodes.

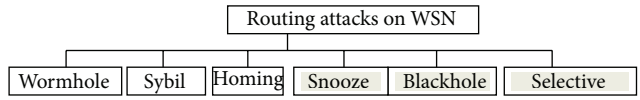

Figure 4: Possible attacks on routing in WSN.

2.3. Security Threats. The dense and unattended deployment of sensor nodes makes it impractical to monitor and protect WSN from physical or logical attack. Karlof and Wagner [5] have identified various security threats to WSN based on the protocol stack. Here we are concentrating mainly on possible threats at routing layer as shown in Figure 4.

Sybil Attack. Douceur [15] has first identified this attack in which the attacker pretends to be at several places at the same time. All those fabricated identities are known as Sybil nodes. The attacker may communicate with legitimate nodes via these Sybil identities and can get access to sensitive information or can affect the normal working of the network.

Wormhole Attack. In Wormhole attack [16] two malicious nodes form a tunnel and one malicious node records the packets at one side of the tunnel while the other malicious node replays them from another point of the tunnel. This tunnel can be formed with the help of a wired or wireless link. It provides a low latency link between two distant nodes. This way the attacker can attract the traffic, then drop them or can perform a man-in-middle attack.

Homing. In this kind of attack, the attacker keeps track of the network traffic and tries to estimate the geographic location of some special nodes like cluster heads or base station. After getting their location they can be damaged physically or can capture their traffic to perform some other harmful attacks like sniffing, attacks on data integrity, and so forth.

Selective Forwarding. In selective forwarding attack, the malicious node does not forward all the data packets coming to it, but it does this selectively; that is, it drops some of the packets and forwards others. This packet drop may happen arbitrarily or periodically.

Blackhole Attack. Blackhole attacker tries to lure the traffic from a particular region by exploiting the loopholes in the routing protocol. After getting the data packets it can drop them.

Snooze Attack. We have identified a new snooze attack [17] on the cluster-based protocol, in which the attacker goes into

the sleep mode when its turn to forward the data packets. An attacker may do it to save its own battery or to not forward the packets of some of the nodes to the base station.

Many researchers have proposed several methods to secure WSNs against various security threats. The following section gives a brief overview of various security solutions proposed in the literature for WSN.

3. Related Work

Several techniques exist in the literature to improve the security of WSN. Some of them are explained below.

In [18], the authors proposed SecLEACH, a method that uses the random key predistribution scheme to secure the LEACH protocol. When the network starts, a key pool of randomly generated keys and IDs are generated. A string of keys selected by the pseudorandom number generator is assigned to various nodes. All the node-to-node communication happens with the help of pairwise keys only. The authors claim that their protocol provides integrity, authenticity, confidentiality, and freshness to node-to-node communication. Their protocol suffers from the problem of orphan node; that is, a node that does not share pairwise key with others in its preloaded key ring cannot participate in any cluster and has to elect itself as cluster head. Orphan nodes increase the overhead of transmission.

In [19], the authors proposed a trust-based method to secure LEACH protocol known as CSLEACH. Each node shares a unique private key with base station which is used for broadcast authentication. They claim that if an attacker tries to become a CH, cluster members invalidate it and its trust would be reduced. This method lacks broadcast authentication, so even a single compromised node can easily perform DoS attack by attacking the synchronization of the network.

In [20] the authors proposed an intrusion detection scheme for sensor networks for selective forwarding attack and sinkhole attack which are variant of blackhole attack. They use Watchdog approach by neighboring nodes to detect the attacks. They apply some rules on every node to jeep a count on the number of messages dropped by that node. An alarm will be produced when their count reaches a threshold. This method is not very efficient method because for the final decision, alerts from all the neighbors have to be received. The measurement of energy is also not taken into consideration during the implementation of this method.

In [21], the authors assume the prior deployment of the sensors in a group and each of the sensors is given a set of randomly selected keys from the large key pool which is used for communication with its group members. In addition every sensor node also has a key to communicate with the BS. With the help of these keys they argue that communication between sensors and BS will be secure. They claimed that in some scenarios their scheme outperforms SecLEACH but the main drawback of their scheme is that it requires prior knowledge of deployment area and any change in topology will change the overall efficiency of the scheme.

All these schemes work towards a secure WSN but none of the methods is robust against all kinds of attacks.

4. Problem Formulation

Our objective for this research is to develop a mechanism that can detect various packet drop attacks in WSN. We have assumed a WSN consisting of N sensor nodes and a base station BS, and the set of nodes is known as $S = \{s_1, s_2 \ldots . s_N\}$. The sensor nodes are sensing the data from the environment and sending it to the base station via a cluster-based routing protocol. We have chosen the cluster-based routing as compared to flat routing because cluster-based routing is more efficient in terms of load balancing and network lifetime [22]. We have used LEACH-C as routing protocol. This protocol selects the cluster heads, which are responsible for data aggregation and forward the aggregated data to the base station. The base station keeps a watch on the data coming from various cluster heads to detect any drop attack. The attack may happen due to the malicious act of an attacker node $S_m \in S$. So the problem is to identify the attacker node S_m from the set S. A base station is having high resources as compared to the sensor nodes so in our method most of the computations are done at base station only.

Base station constructs a vector V_i for each node, which consists of attributes related to node i. We have considered mainly two attributes, one is data sent by node i, D_i, and another is residual energy of node i, RE_i, for drop detection. These attributes are easily available to the base station and they are applicable to other clustering protocols too.

In order to evaluate the effectiveness of our scheme we have simulated it on network simulator NS-2. We have implemented various drop attacks and measured the accuracy of our scheme for the detection of those attacks. We have simulated three types of attacks: blackhole attack, selective forwarding attack, and snooze attack. Since we are using cluster-based routing LEACH-C for our simulations so we have assumed that in all the scenarios the attacker is the cluster head for the current round because it is the node which is responsible for transmitting the data of all of its members.

Now first we describe implementation of these attacks and detection scheme in detail; then we will present the result of our detection scheme.

4.1. Simulated Attacks. We have simulated three packet drop attacks for the LEACH-C routing protocol, which is a popular cluster-based routing for WSN. The attacks simulated are as follows.

Blackhole Attack. In the following section we will explain the blackhole attack and its consequences in WSN. The time depends upon the basic protocol functioning and does not include propagation delays. When there was no attack in the network, the target node A's cluster head, say L, is set as a cluster head in the CHAdv (cluster head advertisement) messages sent by the BS. Nodes receiving these CHadv messages join a cluster with CH (cluster head) as L, which is used to transmit the messages to the BS. During attack,

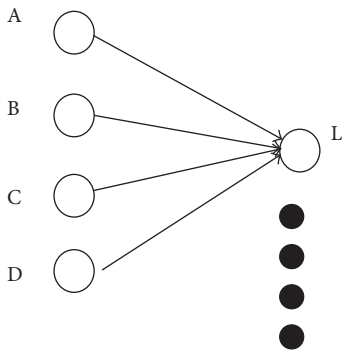

Figure 5: A subset of WSN cluster with node L as attacker and other nodes as victims.

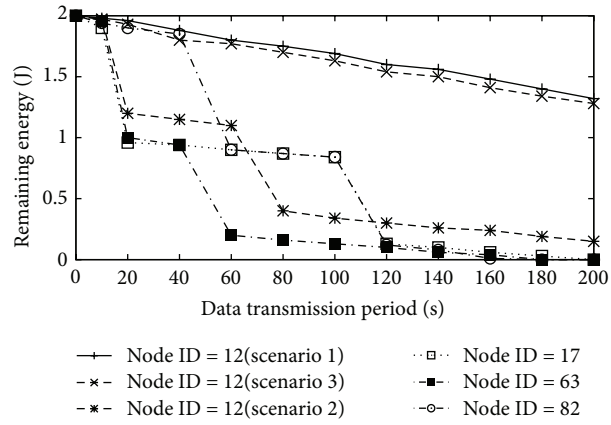

Figure 6: Energy consumption by various nodes in case of attack.

all data messages coming to L through A or other cluster members are dropped as shown in Figure 5. The nodes of this cluster will not be able to communicate with BS. This scenario will remain the same until the cluster head of node A changes.

This is known as round time in case of LEACH-C. At the end of every round time all the nodes send their remaining energy to the BS. Now based on the received energy, BS applies simulation annealing algorithm and finds the cluster heads and their members for the next round. Two cases are there.

Case I: A cluster head L sends its members' data to BS. In this communication, it loses a significant amount of its remaining energy. Due to this method the chance of becoming a cluster head for node L to become a cluster head in next round reduces.

Case II: Cluster head L is receiving the data from its cluster members but not sending any data to BS.

So there is no energy consumption of transmitting the data to BS for node L in Case II. Hence, its remaining energy will be higher as compared to Case I and it again has a chance to become a cluster head for the next round.

We call the abovementioned attack as attack scenario 1.

4.2. Selective Forwarding Attack. In scenario 2, after becoming a cluster head, attacker selectively sends data to base station. Although the effect of this attack is less harmful as compared to blackhole attack because base station is still receiving some data from the attacker, in a long way it may affect the overall observation of the base station. Also, due to selective forwarding of data the attacker detection is difficult in this type of attack

4.3. Snooze Attack. In snooze attack, the attacker is saving more energy because it will be in sleep mode instead of active mode, so its chances of becoming a cluster head in the next round are higher as compared to the previously mentioned attacks. It is very easy to detect because the attacker is becoming the cluster head most of the time but is not sending any data to the base station. This makes attack scenario 3.

5. Packet Drop Detection and Countermeasure

In our scheme we have assumed that all the sensor nodes are aware of their locations by the means of GPS or some other location-aware system. After deployment nodes remain stationary. All the nodes are having same communication and computation capabilities. If the battery of any node is exhausted it is considered dead.

Our scheme is totally relying on the information extracted from the packet sent by the node to the base station. We are not considering any packet modification attacks. The base station is the main monitoring node in our case. So our scheme does not put any extra communication overhead on the resource constraint sensor nodes of the network.

An attacker may physically capture a legitimate node and force it to misbehave through some malicious code or may introduce some compromised node in the network. All the communications are happening in air so an attacker can easily eavesdrop and can bypass some basic security mechanisms.

For each kind of attack when we observed the energy profiles of various nodes, we found that on an average an attacker will have higher residual energy as compared to other nodes as it is not dissipating its energy in communication. From Figure 6 we can observe the difference of residual energy among the other legitimate node and the malicious node (ID = 12).

Similarly we found a measurable difference in amount of data packets sent by various legitimate cluster heads and the attacker. Figure 7 gives the information about data frames sent by various cluster heads at time = 200 sec; here CH2 = node ID 12. On the basis of these observations we formulated our detection scheme. In the rest of the section we will describe our detection technique in detail.

5.1. Vector Formation. In LEACH-C protocol all the cluster members will send their sensed data to respective cluster heads in their TDMA slot. Cluster head aggregates this data and forwards it to the base station. That means base station is getting the data from each cluster head after a time interval t_{round}. After the completion of a round all the nodes will send their residual energy information to the base station to

```
(1) if (t = t_round) then
(2)     if (D_i <= Ø && RES_i > RES_j) then
// where j ∈{CH-i}
(3)         susflag_i = susflag_i + 1
(4)     end if
(5) end if
(6) if (t_round = t_window) then
(7)     if (susflag_i ≠ 0 && CH-Count_i > avg (CH-Count))
(7)         confirm attacker i
(8)         Attacker-list = {Attacker-list} ∪ {i}
(9)     else
(10)        Attack is not confirmed
(11)    end if
(12) end if
```

Algorithm 1: Algorithm for deciding whether the node is attacker or not.

```
(1) if ({i} ∈ Attacker-list) then
(2)     Do not accept any messages
(3) else
(4)     Use their info to form clusters
(5) end if
```

Algorithm 2: Algorithm for avoiding the attacker.

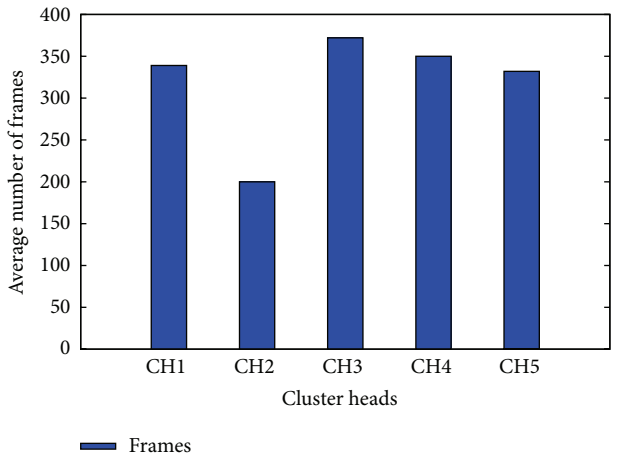

Figure 7: Average number of frames reached at BS in case of attack.

become a cluster head for the next round. The base station has data of all the cluster heads as well as residual energy of all the nodes. So it forms a vector to store this information for all the nodes which consist of D_i, RES_i, and CH-Count_i where CH-Count_i is the counter for number of times a node elected as cluster head.

5.2. Attack Detection. Our aim is to detect drop attacks in WSN. Base station forms the vectors as described above and then it watches the behavior of various nodes for a window of 5 rounds and then it takes the decision about the malicious node. We will first describe a general algorithm for this and then we will see how it is used to identify the various attackers in different scenarios. Symbols used in the algorithms are as follows: CH is the set of cluster heads for current round, t_{window} is the window time of observation by the base station, and Ø is the threshold for the number of frames received at BS (Ø = 0 in case of blackhole and snooze attack).

The concept here is that a node consumes most of its energy in sending data to the base station and in cluster-based algorithm, this task is performed by cluster heads only. So the residual energy of a CH will be higher as compared to other CHs if it is not transmitting the data at all or doing transmissions in a selective manner. The criterion to become CH is depending on the residual energy of a node, so a node with higher energy will have a high probability to become a cluster head. Based on the amount of data received by a node and the number of times it becomes cluster head in the past due to high residual energy base station will identify the attacker. The various stages of attacker node are shown in Figure 8.

5.3. Countermeasure. After identification BS keeps the IDs of all the attackers in a separate vector called attacker list so in the next round it will not allow the attacker to participate in the network functioning. Algorithm 2 describes the countermeasure.

6. Evaluation

We have analyzed the effectiveness of our scheme by comparing the performance of the network with and without attack

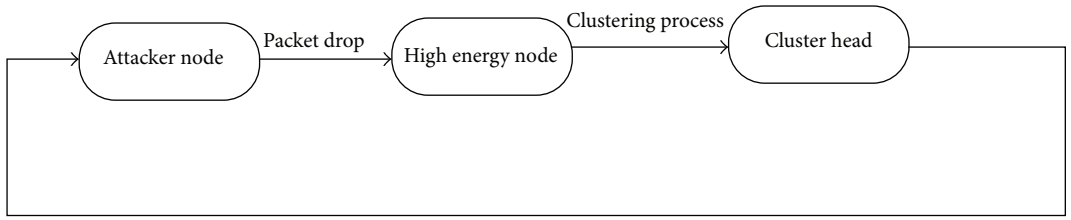

Figure 8: Approach to detect the attacker.

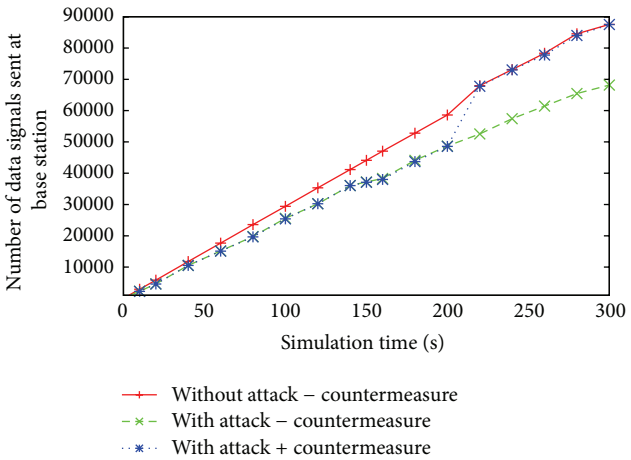

Figure 9: Number of data signals received at BS versus time.

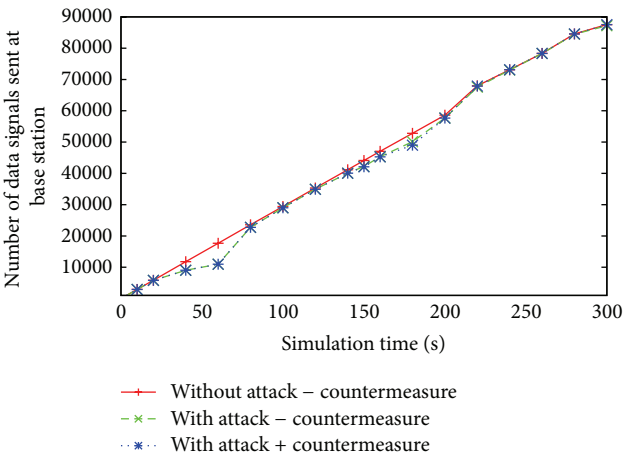

Figure 10: Number of data signals received at BS versus Time.

scenarios. An important issue for the use of this scheme is how to set the parameter t_{window}, as there is a tradeoff between the detection rate and false positive rate. If we have larger value for t_{window} then the attacker may harm our network more and if we choose a much smaller value then legitimate nodes can be identified as the attacker. The optimum choice of w may vary depending on the size and topology of the sensor network. An issue for further research is to test the sensitivity of the choice of w for different network scenarios. For our simulations we have set $t_{\text{window}} = 10 * t_{\text{round}}$. The network was made up of 100 nodes randomly deployed in an area of $100 \times 100\,\text{m}^2$. The number of cluster heads was 5% of the total number of nodes in the network. The number of attackers varied from 1 to 5 depending upon the scenario. For each scenario we have run the simulation for 20 times and the average of them is considered for the graph generation.

For each type of attack, we repeatedly tested the accuracy of our scheme using different values of the window time w from Algorithm 1 and we found the acceptable results for $10\times t_{\text{window}}$. From Figure 9, it is clear that in case of snooze attack or blackhole attack the data delivered to the base station will be less as compared to those without attack scenario but after our countermeasure is applied, since the attacker is not allowed to participate in the network, so normal delivery of data takes place after 200 sec.

In case of selective forwarding attack the difference of data which reached the base station will be less as compared to the blackhole and snooze attack because the attacker is

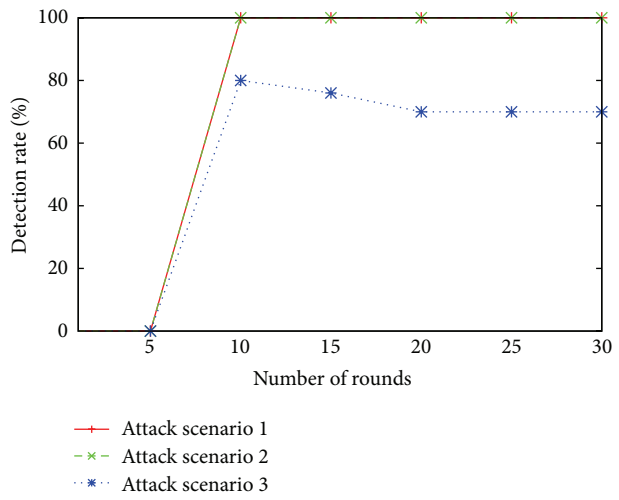

Figure 11: Detection rate for different number of rounds.

not dropping all the packets but it is performing the drop in arbitrary manner. As shown in Figure 10, the effect of attack was more visible at time 40; that is, the attacker was a cluster head at this time and dropped the packets completely but after 200 sec. BS has removed it from the network and the network starts functioning normally.

Figure 11 indicates the correct verdict by our scheme throughout the duration of 600 sec (each round is of 20 seconds) for all three kinds of attacks. BS station confirmed

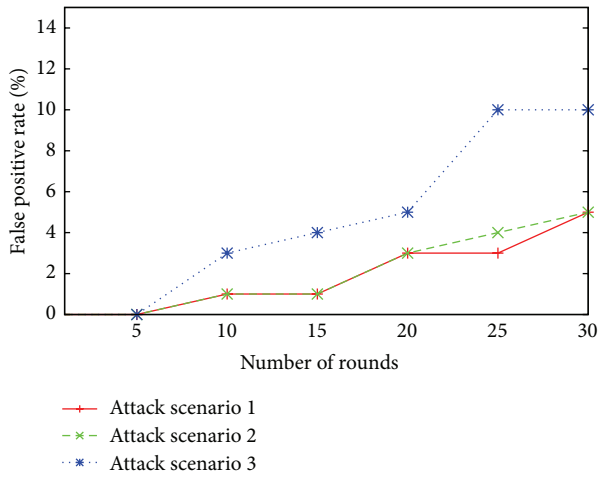

Figure 12: False positive rate for different number of rounds.

the attacker after 10 rounds of the simulation, so there is a horizontal line between 0 and 5. Figure 11 also shows that for blackhole and snooze attack we could get the 100% detection rate, but maximum value of detection rate for selective forwarding attacking was 85% only because of the varying behavior of the attacker.

As observed from Figure 12 the false positive rate (FPR) was also higher in case of selective forwarding attack. This is because some of the legitimate nodes could not meet the data threshold as they are having less number of cluster members in their clusters due to which they are also identified as attacker. In case of snooze attack the difference of energy and data values were clearly visible in simulations so it was easily identified as compared to balckhole attack.

Our scheme is energy efficient as no extra burden for detection of attacker is put on the sensor nodes. All the complex tasks are handled by the base station which is a highly resourceful node.

7. Conclusion

In wireless sensor networks security is always a critical issue for the researchers. Through this paper, we have made three important contributions. One is we have identified the drop attack detection scheme from the perspective of base station. Secondly we have extended the simulator to show the effect of attacks as well as to validate the effectiveness of our detection scheme on various drop attacks. Third after detection of the attacker we were able to remove it from the network successfully with much less overhead. One promising direction for further improvement in our work can be to add some authentication mechanisms at base station to prevent spoofing attacks. There is also a scope of research for inclusion of base station to detect other kinds of routing attacks. Another possibility for future work is securing the base station from the attackers.

References

[1] K. Sohraby, D. Minoli, and T. Znati, *Wireless Sensor Networks Technology, Protocols, and Applications*, John Wiley & Sons, New York, NY, USA, 2007.

[2] T. Bokareva, W. Hu, S. Kanhere et al., "Wireless sensor networks for battlefield surveillance," in *Proceedings of the Land Warfare Conference*, Brisbane, Australia, 2006.

[3] F. Ingelrest, G. Barrenetxea, G. Schaefer, M. Vetterli, O. Couach, and M. Parlange, "SensorScope: application-specific sensor network for environmental monitoring," *ACM Transactions on Sensor Networks*, vol. 6, pp. 1033–1047, 2010.

[4] A. Garcia-Sanchez, F. Garcia-Sanchez, F. Losilla et al., "Wireless sensor network deployment for monitoring wildlife passages," *Sensors*, vol. 10, no. 8, pp. 7236–7262, 2010.

[5] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: attacks and countermeasures," *Special Issue on Sensor Network Applications and Protocols*, vol. 1, no. 2-3, pp. 1293–1303, 2003.

[6] W. R. Heinzelman, J. Kulik, and H. Balakrishnan, "Adaptive protocols for information dissemination in wireless sensor networks," in *Proceedings of the 5th annual ACM/IEEE international conference on Mobile computing and networking*, pp. 174–185, Seattle, Wash, USA, 1999.

[7] D. Braginsky and D. Estrin, "Rumor routing algorithm for sensor networks," in *Proceedings of the 1st ACM International Workshop on Wireless Sensor Networks and Applications (WSNA '02)*, pp. 22–31, Atlanta, Ga, USA, September 2002.

[8] C. Intanagonwiwat, R. Govindan, and D. Estrin, "Directed diffusion: a scalable and robust communication paradigm for sensor networks," in *Proceedings of the 6th Annual International Conference on Mobile Computing and Networking (MOBICOM '00)*, pp. 56–57, New York, NY, USA, August 2000.

[9] C. Qing, T. Abdelzaher, H. Tian, and R. Kravets, "Cluster-based forwarding for reliable end-to-end delivery in wireless sensor networks," in *Proceedings of the 26th IEEE International Conference on Computer Communications (INFOCOM '07)*, pp. 1928–1936, San Diego, Calif, USA, May 2007.

[10] W. R. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "Energy-efficient communication protocol for wireless microsensor networks," in *Proceedings of the 33rd Annual Hawaii International Conference on System Siences*, pp. 3005–3014, January 2000.

[11] A. Manjeshwar and D. P. Agrawal, "A protocol for enhanced efficiency in wireless sensor networks," in *Proceedings of the 1st International Workshop on Parallel and Distributed Computing Issues in Wireless Networks and Mobile Computing, in Conjunction with 2001 IPDPS*, San Francisco, Calif, USA, 2001.

[12] S. Lindsey and C. S. Raghavendra, "PEGASIS: power-efficient gathering in sensor information systems," in *Proceedings of the IEEE Aerospace Conference*, pp. 1125–1131, Big Sky, Mont, USA, March 2002.

[13] W. B. Heinzelman, A. P. Chandrakasan, and H. Balakrishnan, "An application-specific protocol architecture for wireless microsensor networks," *IEEE Transactions on Wireless Communications*, vol. 1, no. 4, pp. 660–670, 2002.

[14] T. Murata and H. Ishibuchi, "Performance evaluation of genetic algorithms for flowshop scheduling problems," in *Proceedings of the 1st IEEE Conference on Evolutionary Computation*, pp. 812–817, June 1994.

[15] J. R. Douceur, "The sybil attack," in *Proceedings of the Workshop on Peer-to-Peer Systems (IPTPS '02)*, Cambridge, Mass, USA, 2002.

[16] Y. C. Hu, A. Perrig, and D. B. Johns, "Wormhole attacks in wireless networks," *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 2, pp. 370–381, 2006.

[17] M. Tripathi, M. S. Gaur, and V. Laxmi, "Simulation of Snooze attack in LEACH," in *Proceedings of the 3rd International Conference of Computer Science, Engineering and Applicaions (ICCSEA '13)*, pp. 393–399, New Delhi, India, May 2013.

[18] L. B. Oliveira, A. C. Ferreira, and M. Aurelio, "SecLEACH-on the security of clustered sensor networks," *Signal Processing*, vol. 87, no. 12, pp. 2882–2895, 2007.

[19] L. Yang, *Centralized security protocols for wireless sensor network [M.S. thesis]*, San Jose State University, 2011.

[20] K. Ioannis and T. Dimitriou, "Toward intrusiondetection in sensor networks," in *Proceedings of the 13th European Wireless Conference*, pp. 1–7, April 2007.

[21] P. Banerjee, D. Jacobson, and S. N. Lahiri, *Performance and security measure of clustering protocols for sensor networks [Ph.D. thesis]*, Iowa State University, Ames, Iowa, USA.

[22] S. Pal, D. Bhattacharyya, G. S. Tomar, and T. Kim, "Wireless sensor networks and its routing protocols: a comparative study," in *Proceedings of the International Conference on Computational Intelligence and Communication Networks (CICN '10)*, pp. 314–319, November 2010.