Jamming Detection Mechanisms for Wireless Sensor Networks

Murat Çakıroğlu
Sakarya University
Technical Education Faculty
Electronics/Computer Department
+90 264 2956456
muratc@sakarya.edu.tr

Ahmet Turan Özcerit
Sakarya University
Technical Education Faculty
Electronics/Computer Department
+90 264 2956450
aozcerit@sakarya.edu.tr

ABSTRACT
The Jamming-style Denial of Service (J-DoS) attacks are significant causes of malfunctioning of Wireless Sensor Networks (WSNs). The nodes of WSNs are prone to external disturbances especially when they are used in hostile environments. The attackers mainly operate in the wireless communication medium by following a couple of diverse scenarios. In this paper, we have developed two detection mechanisms used for J-DoS attacks in order to differentiate the legitimate and adversary scenarios. The detection mechanisms designed utilize some network parameters and additional packets to separate and classify normal conditions and adversary ones. Having detected the type of the attacker, appropriate counter measures can be applied.

Categories and Subject Descriptors
C.2.0 [**Computer-Communication Networks**]: General – Security and Protection

General Terms
Anomaly Detection, Security, Algorithm

Keywords
WSN, DoS attacks, MAC, Jamming detection

1. INTRODUCTION
WSNs consist of sensor nodes with limited capacity, low cost and communicating with each other in short distances using considerably low power rate [1]. WSNs are mostly scattered randomly into the target field and they execute a common strategy to transfer pre-specified parameters of the environment to the base. Because of their wide range of functions, they can be used in many diverse applications ranging from military fields to health services.

In most cases, sensor nodes function in relatively harsh environments and therefore, they have a high risk of physical damages compared to conventional networks. For example, the cryptographic keys can be obtained by a saboteur and the nodes can be reprogrammed to destroy whole ongoing communication in the network [4,10]. The security weaknesses of the sensor networks can be exploited further to create many types of threats.

The J-DoS attackers emit radio signals into the communication medium by following many types of scenarios in order to disrupt ongoing network activities [6]. There have been many numbers of research activities in this topic. Firstly, collision, exhaustion and unfairness types of attacks were introduced [6] and then constant, deceptive, random and reactive jammers were presented [6]. Later, energy efficient jammers were described in [5, 8] for various types of MAC protocols and energy efficient four types of new jammers were also introduced in [14]. However, the MAC and physical layer jamming detection methods are rarely studied.

Xu et al. have developed two distinct algorithms to detect the existence of a jammer [6]. In the first algorithm, Packet Delivery Ratio (PDR) and Received Signal Strength Indication (RSSI) dispersion ratios are used to distinguish the legitimate operations from the jammed ones. Various numbers of scenarios were applied to measure the PDR values corresponding to the RSSI values. In doing so, appropriate threshold signal levels are sampled so that two distinct regions can be determined: benign-region and jammed-region. If any node has the PDR parameter lower than threshold value and RSSI parameter higher than RSSI threshold level, an attack is assumed. The major disadvantage of this method is that the system is tested by only three nodes: a transmitter, a receiver, and a jammer. Especially in large scaled and high density networks the collision rates can be augmented because of high number of neighbor nodes and the RSSI parameter, which is used to separate the benign and jammed regions from each other, cannot be easily determined [9]. Thus, the detection performance of this method can be considerably decreased.

In the second method proposed by Xu et al., the PDR values and the location data of the nodes are utilized for detection procedures. Yet, this method requires some additional GPS (Global Positioning System) hardware or localization techniques. Another detection mechanism for jamming attacks was suggested by Wood et al. [3]. There, the attackers can be identified by the channel utilization rate that is lower than a specified threshold level. However, the channel utilization rate can also be decreased by the failures originated from hardware and software faults of the surrounding neighbor nodes. The channel utilization rate, therefore, cannot be used alone to determine the presence of an attack.

INFOSCALE 2008, June 4-6, Vico Equense, Italy

DOI 10.4108/ICST.INFOSCALE2008.3484

In this study, we have designed the AJDA (Anomaly based Jamming Detection Algorithm) mechanism to detect jamming style attacks. The contributions of this research paper are:

- Isolating jamming style attacks from natural network conditions such as collision, hardware, and software faults maintaining high detection rate and low false positive rate.
- Wide-ranging and lightweight detection mechanism for various types of attacks.
- No additional hardware (DSP etc.) requirement for detection mechanisms

The rest of the paper is organized as described below. Jammer models are introduced in Section-2. The problem definition and jammer detection criteria will be clarified in Section-3. In Section-4 and Section-5, the basic and advanced algorithms are revealed. Simulation assumptions are described in Section-6 and simulation results are discussed in Section-7. The paper is concluded by Section-8.

2. OVERVIEW OF JAMMER MODELS

There are a number of jammer types, which were studied before, affecting physical and medium access layer functions. Xu et al. [8] have defined four attacker models: constant, deceptive, random, and reactive. Law at al. has also suggested four jammer models for S-MAC protocol: periodic cluster, listen interval, control interval, and data packet jammers [5, 8]. Wood et al. has contributed to jammer models by describing interrupt, activity, scan, and pulse jammers [12].

2.1 Constant Jammer

The jammer sends out random bits to the communication medium following chaotic protocol rules. The communication among the nodes is suspended by these activities. However, this type of attackers are not energy efficient, therefore, they are not right choice for applications with limited power.

2.2 Deceptive Jammer

Instead of sending out random bits constantly, the deceptive jammer transmits the legitimate packets to the medium at high rates. In this manner, nodes remain in receiving mode constantly and thus, the communication medium is kept unavailable all the time. Since it attacks persistently, the deceptive jammer is not energy efficient as well.

2.3 Random Jammer

The random jammer attacks the network at random time slots, and sleeps in the rest of periods. The random jammer imitates the constant or deceptive jammer; however, it is somewhat more energy efficient compared to them.

2.4 Reactive Jammer

It always listens to the medium. The reactive jammer place an attack when any communication is initiated in the medium. Legitimate packets sent out by sensor nodes get corrupted in this way. Since the reactive jammers listens to medium constantly, they are not energy efficient. However, they are not easy to be detected.

2.5 Periodic Listening Interval Jammers

Law et al. have discovered that there is a strong possibility for the implementation of various attacking scenarios by making use of S-MAC's constant timing structure. In Figure-1, the periodic timing diagram of the SMAC is shown. Since no encryption mechanism is used in S-MAC protocol, the details of the data packets can easily be revealed. By the help of the SYNC packets, the listen/sleep periods can be predicted. Energy efficient attackers synchronized with the sensor nodes can be designed in this manner. Law et al. have developed three distinct energy efficient jammer types by making use of this disadvantage. Periodic listening interval jammer attacks when the nodes are in listening period and sleeps at all times.

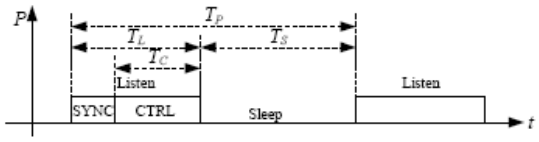

Figure-1 S-MAC timing diagram.

2.6 Periodic Control Interval Jammer (PCIJ)

The PCIJ first analyzes the ongoing communication and then calculates the control (CTRL) slots in the data frames by using statistical methods. The PCIJ attacks when the nodes are in CTRL period and sleeps the rest of the times.

2.7 Periodic Data Packet Jammer (PDPJ)

The PDPJ listens to the channel in the CTRL interval and it attacks the data segment when a CTS segment is encountered. The jammer remains in sleep mode in the rest of the times.

2.8 Periodic Cluster Jammer

Law et al. have designed another attacker model to be used for the nodes that communicates each other with encrypted packages [5]. The jammer model conducts a couple of statistical estimation on encrypted packets and determines the timing of the data segment of the frame. Jammer can identify the data segments from the fact that they are always longer than the control segments. Two or more virtual cluster having disparate listen/sleep mode timing may exist in the jammer's environment and the arrival time of the packages can be intermingled in this circumstance. In order to overcome this obstacle, periodic cluster jammer employs K-means clustering algorithm to separate each cluster [5].

2.9 Interrupt Jammer

Instead of remaining in listening mode steadily, the interrupt jammer remains in passive listening mode. The jammer awakens and conducts an attack by means of a hardware interrupt when a preamble and a start of frame delimiter (SFD) are detected in a packet.

2.10 Activity Jammer

If the packet is encrypted, the interrupt jammer cannot recognize the preamble and the SFD. In such conditions, the activity jammer initiates an attack to the medium assuming an ongoing communication between nodes if the RSSI level is higher than the threshold level.

2.11 Scan Jammer

The scan jammer uses a technique against alert nodes in the network utilizing the channel hopping mechanism. Instead of detecting a packet in a single channel, the scan jammer searches out all possible channels for a packet in a period of time. On success, an attack is initiated in the regarding channel.

2.12 Pulse Jammer

Packet segmentation along with channel hopping is another defense strategy against scan jammers. To overcome this strategy, the pulse jammer remains on a single channel and sends out small packets constantly to block the ongoing communication.

3. THE PROBLEM DEFINITION AND JAMMING DETECTION CRITERIA

The jamming attacks can result in abnormal conditions by impeding or blocking the communication in the sensor network. A number of network parameters such as increase on collision rate, bad frame rate, and the RSSI level along with medium access difficulties suggest that there may be an attack against the network conducted by a jammer. While abnormal parameter values can be considered as an attack alert, they can also be caused by natural network conditions. For example, congestion, hardware or software faults in the sensor nodes or changes in the environment may also trigger conditions similar to scenarios caused by jammers.

As articulated in Section-2, smarter attacking methods and limited hardware in the sensor nodes could complicate to initiate a counter attack against the jammers. In this paper, we have implemented two successive algorithms to separate natural network conditions from the harmful ones requiring no additional hardware or unit. The algorithms designed utilize and analyze some system parameters obtained from MAC and physical layers.

3.1 Packet Delivery Ratio (PDR)

The PDR is the ratio of the number of delivered packets compared to the number of sent out packets. A sender node confirms the deliverance of a packet only upon receiving an ACK packet from a receiver node. If 4-ways handshaking (RTS/CTS/DATA/ACK) mechanism is used, the PDR can be found by comparing of the RTS and DATA packets to be sent in response to the CTS and ACK packets to be received. The PDR parameter is not only decreased by a jammer, but also decreased significantly by imperfect connections, faults in the neighbor nodes, and collisions. Therefore, the PDR cannot be used alone to discriminate natural network conditions from the symptoms of the attacks.

The maximum, minimum and average PDR values of a sensor node under attacks of various jammers can be seen in Figure-2 with 60 seconds intervals. Reactive and interrupt jammers corrupt most of the control or data packets. On the other hand, since constant, deceptive, listen and control jammers occupies the communication medium all the time, they impede the sensor nodes from sending any packets, in consequence, the PDR value cannot be acquired higher than zero.

Random jammers attack the network at random time slots and can damage the data or control packets. However, the cluster and data packet jammers only attack to the data packets. These jammers can cause the PDR values to decrease considerably. The effectiveness of the activity jammer is related to jammers' sensing ability for a valid communication in the channel in a proper way. If the activity jammer operates in a noisy channel, the effectiveness of it can be dropped significantly. Scan jammers, on the other hand, test all possible communication channels and therefore, they are not usually fast enough to destroy communication in all channels. So, the PDR levels in scan jamming attacks cannot be affected as anticipated. In contrast, pulse jammer remains on a single channel and sends out jamming packets into that channel. Therefore, pulse jammers are much more effective than scan jammers in terms of the dropping of PDR levels.

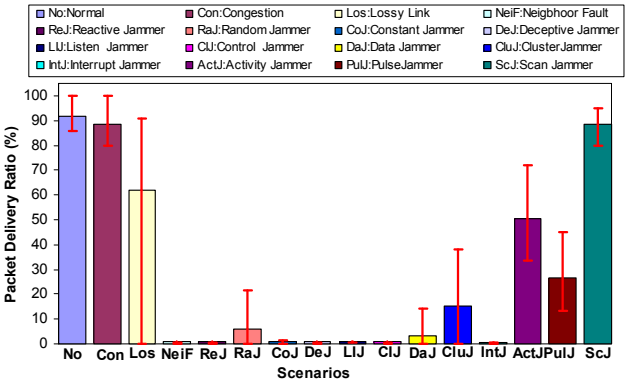

Figure-2. The average PDR ratios sampled in a sensor node with diverse attacking scenarios (Sampling period: 60sec., simulation length: 36000 sec., error bars indicate the maximum and minimum values).

3.2 Bad Packet Ratio (BPR)

The BPR is the ratio of the number of erroneous packets compared to the number of received total or preamble packets for a sensor node. Sensor nodes determine the robustness of packets by using the CRC test and drop the packets if the CRC test result is negative. The PDR and BPR parameters demonstrate the quality of communication for transmitter side and receiver side respectively. These two parameters are in inverse proportion in most cases; however, both the BPR and PDR parameter values can be low in particular cases.

In Figure-3, sensor node-B and node-C are supposed to be under attack of a reactive, interrupt or activate jammer. In this case, the PDR value of these nodes will be low; however, the BPR value will be high. When the nodes are under attack of a constant, listen interval or control interval jammers, node B and node C cannot transmit or receive packets because of uninterruptedly busy communication channel occupied by jammers. In such a scenario, the BPR and PDR values of the node-A (boundary node) may be low, since node B can not send ACK packet to node A because of uninterruptedly busy channel. Thus, node A is affected from the jamming. But under the reactive, random, interrupt, activate, scan, pulse, data packet and cluster jamming scenarios, the jammers can not corrupt the reception or transmissions of node B since it is just inside the border area of jammers.

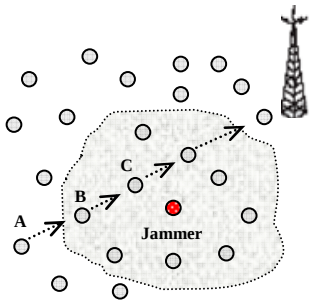

Figure-3. A Jamming Scenario.

The BPR values sampled in diverse scenarios can be seen in Figure-4. In most attacking scenarios, the BPR values are considerably higher than the values caused by natural network causes. These occurrences can be used to separate jamming scenarios from the natural network failure scenarios. On the other hand, the BPR value can be obtained as zero if constant, listening and control interval jammers in action where there is no valid packet or preamble received by the node. Such attacking scenarios complicate to identify the cause of low level BPR and PDR values.

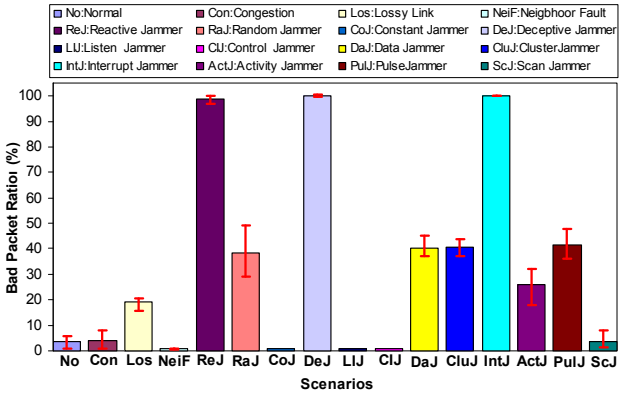

Figure-4. The maximum, minimum and average BPR values obtained from a node with diverse scenarios (Sampling period: 60sec., simulation length: 36000 sec., error bars indicate the maximum and minimum values).

3.3 Energy Consumption Amount (ECA)

The ECA is defined as approximated energy amount consumed in a specified time for a sensor node. The radio unit of a MICA2 node consumes 16,5mA, 9,6mA, and 1μA in transmit, receive, and sleep modes respectively [14]. It means that with a 3v battery, the radio unit of the MICA2 node dissipates 49,5mW, 28,86mW, and 3μW power in transmit, receive, and sleep modes respectively. The estimated power dissipation of a MICA2 node can be calculated for a specified time by using the operating period of radio unit and power dissipation factors given above.

The average energy consumption rates obtained from a node at 60 seconds intervals are illustrated in Figure-5. Deceptive, constant, random, listen interval, and control interval jammers cause sensor nodes to consume considerably more power. Sensor nodes under attack of deceptive jammer are held in receive mode, whereas they are held in listen mode when the attacks are originated from constant, listen interval or control interval jammers. Constant, listen interval, and control interval jammers force sensor nodes to remain in BACKOFF period by occupying the communication channel constantly and the nodes continue to remain in listen mode, even if they are released from the BACKOFF period in the sleep mode. Therefore, the nodes in BACKOFF period cannot be shifted into sleep period and this constraint cause the nodes to run out their batteries earlier. Since there is no IDLE mode in the CC1000 radio unit, the nodes dissipate equivalent power under attack of constant, listen interval, control interval, and deceptive jammers. The nodes under attack of random, constant, deceptive, listen interval, control interval jammers consume more power than normal network scenarios and this consequence can be used to distinguish the normal and jamming scenarios from each other.

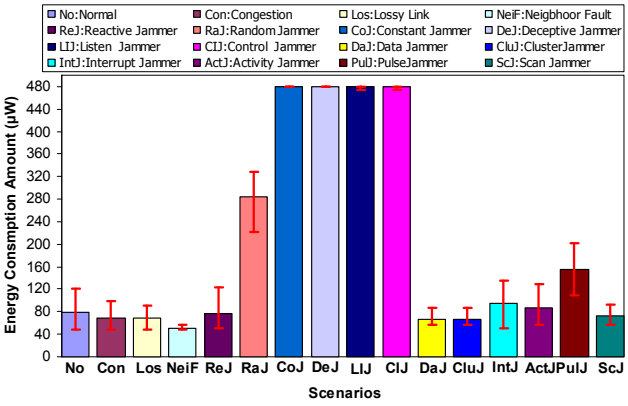

Figure-5. The maximum, minimum and average energy consumption values obtained from a node with diverse scenarios (Sampling period: 60sec., simulation length: 36000 sec., error bars indicate the maximum and minimum values).

4. THE PROPOSED BASIC JAMMING DETECTION METHOD

An anomaly based jamming detection method has been developed by utilizing parameters, which are detailed in Section 3. In this method, system behaviors are classified in order to create an initial system profile and abnormalities in the sensor network can be identified by comparing later profiles. The initial parameter levels (PDR, BPR, and ECA) are sampled in the installation phase and it is assumed that no jammer can disturb the sensor network. The sampled and recorded threshold levels are used later to detect the existence of any jammer.

The 6-Sigma method, which is a simple yet an efficient calculation technique, has been used to determine the threshold levels. In this method, the UCL (Upper Control Limit) and the LCL (Lower Control Limit) limits of normally distributed samples can be calculated by the help of the arithmetic mean and standard deviation values (Equation 1, 2). The arithmetic mean is represented by μ and σ stands for standard deviation. In normally distributed outputs, 99.999660% of the data are between the UCL and the LCL limits. The rest of the data set, which are lower than the LCL or higher than the UCL, are regarded as abnormal levels as shown in Figure-6.

$$UCL = \mu + 6\sigma \qquad (1)$$

$$LCL = \mu - 6\sigma \qquad (2)$$

The LCL is used for the determination of PDR threshold values; on the other hand, the UCL is used for the determination of the BPR and ECA threshold levels.

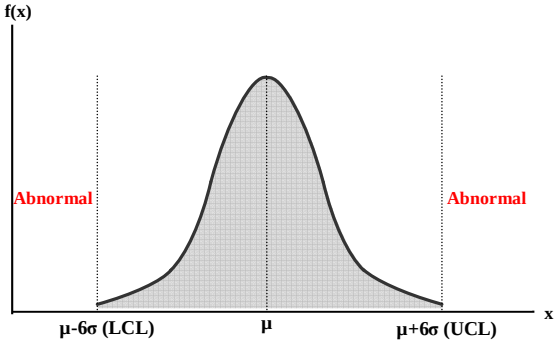

Figure-6. Calculation of the threshold values by the help of 6 sigma method.

The pseudo codes of the basic jamming detection mechanism are given in Algorithm-1 in which recorded parameters threshold values are compared to periodic measurement of these parameters. The attacks and fault cases are classified by five-branched if-else statements. Each branch corresponds to one or more attack types or a fault case. For example, in the first query code line a sensor node is accepted under attack when instant PDR is lower than the threshold value (PDR_{The}) and instant ECA is higher than the threshold and instant BPR is higher than the threshold.

Algorithm 1. Basic Jamming Detection Mechanism

```
/* Called every sampling period */
BasicJammingDetectionAlgorithm()
{
  if (PDR<PDRThr AND ECA>ECAThr AND BPR>BPRThr)
     JAMMING=TRUE     // DeJ,RaJ,PulJ
  else if(PDR<PDRThr AND ECA>ECAThr AND BPR<BPRThr)
     JAMMING=TRUE     //CoJ,LIJ,CIJ
  else if(PDR<PDRThr AND ECA<ECAThr AND BPR>BPRThr)
     JAMMING=TRUE    //ReJ,DaJ,CluJ,IntJ,ActJ
  else if(PDR<PDRThr AND ECA<ECAThr AND BPR<BPRThr)
     JAMMING=FALSE  //Boundary node or Fault case
     FAULT=TRUE;
  else if (PDR>PDRThr)
    JAMMING=FALSE
  end if
}
```

The success of the Algorithm-1 depends on determination and measurement of the threshold values. The detection mechanism can generate inappropriate results when sensitive or inaccurate threshold samples are used. Therefore, in some unusual and unexpected network conditions, basic jamming detection mechanism can cause decreased detection rates along with increased false positive rates. There are also some circumstances that an attack or a fault in the sensor network cannot be readily resolved. As shown in Figure-3, Node-A (boundary node) is not directly under attack of a jammer but instead, it is indirectly affected by neighbor nodes. In such scenario; while the PDR value decreases, the ECA and BPR values may remain between typical limits. This difficulty can also appear in case of neighbor node failures. Thus, in the basic detection mechanism, the attack cases and fault cases in the boundary nodes cannot be easily differentiated from each other.

5. THE PROPOSED ADVANCED JAMMING DETECTION METHOD

An advanced jamming detection mechanism is required because of the disadvantages of the basic detection mechanism which are described above. In order to achieve higher detection rates along with lower false positive rates, another supplementary approach is required to support threshold technique. In the advanced mechanism, a query based jamming detection method is developed by the help of the parameters used in the basic jamming detection method and additional network query packets. The advanced detection method not only depends on the relationship of sampled parameters in a node, but also inquires the parameters of neighbor nodes. It is based on exchanging QUERY and REPLY packets between neighbor nodes when abnormal network parameters ($(PDR<PDR_{The}$ && $ECA>ECA_{The}) \| (PDR<PDR_{The}$ && $BPR>BPR_{The})$) are sampled. The sensor node under suspicious condition sends out QUERY packets by setting the ALARM flag in the QUERY packet to determine the existence of an attack. The nodes that receive the QUERY packets examine their network parameters and if any abnormality is met, the ALARM flag in the REPLY packet is set or cleared in otherwise. The nodes can determine the existence of a potential attack by checking the ALARM flags in the QUERY-REPLY packets.

The advanced detection method is implemented by Algorithm-2 given below. **`QueryBasedJammingDetectionAlgorithm`** function is called every sampling period and it uses some external variables and flags to determine the detection of an attack. A QUERY procedure is initiated when an abnormality is met. In order to reduce the QUERY-REPLY packet traffic between the nodes in the same neighborhood, the node received a QUERY packet before sending the QUERY packet should postpone the QUERY sending and waits for REPLY procedure finished. If the numbers of REPLY packets are lower than expected number, the node then sends a QUERY packet. Otherwise, the node does not send a QUERY packet and determine the existence of an attack according to received REPLY packets. The node not received a QUERY packet before sending the QUERY packet must be sent the QUERY in three sampling period by complying with contention protocol rules. If the node cannot send out any QUERY packet in the specific time, it assumes that constant or deceptive jammers occupy the channel. The node sending out the QUERY packet waits for the REPLY packets in a specified time. When the QUERY-REPLY session expires, the nodes examine the REPLY packets to investigate the attacking presence. Nodes determine the existence of a jammer. If:

- No REPLY packet is received
- The numbers of received REPLY packets are lower than the numbers of neighbors and no REPLY packet is received from next hop neighbor
- The numbers of received REPLY packets are lower than or equal to the numbers of neighbors, and an ALARMed REPLY packet is received from the next hop neighbor

Algorithm.2 Advanced Jamming Detection Mechanism.

```
//Called upon each sampling period
QueryBasedJammingDetectionAlgorithm(){
  if ((PDR<PDR_Thr  AND ECA>ECA_Thr) OR (PDR<PDR_Thr and BPR>BPR_Thr))   //Abnormality
    if(RcvdQuery=TRUE  AND WaitingReplyForOtherNodes=FALSE)
       SetReplyTimer(Now+3*SamplingPeriod)
       WaitingReplyForOthers=TRUE
    else if (WaitingReplyForOthers=TRUE AND QueryTimerOverflow=TRUE
       EvaluateReplyPackets();
    else if(RcvdQuery=FALSE  AND WaitingReplyForOtherNodes=FALSE)
      if (TryingToSendQuery=FALSE)
         TryToSendQueryPacket();
         SetQueryTimer(now+3*SamplingPeriod)
         TryingToSendQuery=TRUE
      else if(QueryTimerOverflow=FALSE AND QueryWasSent=TRUE)
         CancelQueryTimer()
         SetReplyTimer(Now+3*SamplingPeriod)
      else if (QueryTimerOverflow=TRUE AND QueryWasSent=FALSE)
         JAMMING=TRUE;
         if(NumberForcedQuery<3)
            SendForcedQuery(now+randomTime)
            ForcedQueryWasSent=TRUE
           NumberForcedQuery++
         end if
      else if(ReplyTimerOverflow=TRUE)
          EvaluateReplyPackets();
      else if (PDR<PDR_Thr  AND BPR<BPR_Thr  AND ECA_n<ECA_Thr  AND RcvdForcedQuery=TRUE)   // Boundary Nodes
          JAMMING=TRUE;
      else if(PDR<PDR_Thr  AND BPR<BPR_Thr  AND ECA<ECA_Thr)
          FAULT=TRUE;
      else
          JAMMING=FALSE;
      end if
    end if
  end if
}
```

In the jamming detection under constant, listen interval and control interval jammers, some special properties are required for boundary nodes. The PDR, BPR, and ECA parameter levels will be low for boundary nodes, which are located on the border of a jammer's coverage area as seen in Figure-3. These parameter levels can also appear in case of neighbor node failures. Therefore, an attack scenario and a fault scenario can be confused. To overcome this drawback in the proposed advanced detection method, the nodes utilize the FORCED QUERY packets. If the node cannot send out any QUERY packet in a specified time, it assumes itself as jammed and waits for a random time to send out a FORCED QUERY packet without complying with contention protocol rules. Therefore, the boundary nodes receiving the FORCED QUERY packet can differentiate the fault or jamming cases more easily.

6. SIMULATION SETUP AND ASSUMPTIONS

In this study, the detection mechanisms for all types of jammers and the realization phase of the algorithms have been implemented in OMNET++ [9] discreet event based simulation environment. 100 healthy sensor nodes along with a sink node, which is located at center, are scattered randomly into a 500x500m^2 of area. To examine the relationship between the number of attackers and the performance of detection mechanisms, four scenarios have been simulated with different ratio of jammed nodes: 25%, 50%, 75%, and 100%. The power rates, power consumptions, and radio distance of normal nodes and jammer nodes are identical and all specifications comply with the MICA2 [11] sensor node. S-MAC [2] protocol has been chosen for MAC layer and duty cycle of the MAC configured as 10% (100ms for listen, 900ms for sleep). In each simulation, the sensor network has been assumed to operate in a proactive manner, or in other words, all sensor nodes send out periodic report to the sink node. For typical traffic loads 1 packet for 5 second and for heavy traffic loads 2 packets for 1 second have been selected. In order to investigate the fault conditions of the nodes, randomly selected 25% of nodes have been artificially forced to faulty status at random intervals.

In WSNs basic radio devices are usually preferred to decrease both the cost and power consumption of the nodes. In our simulations, we have preferred to use two event discreet Markov chains [13] since the radio unit provides either good or bad

transmission service. This model is also called Gilbert-Elliot model that is used for simulating transmission losses. The PDR, BPR, and ECA parameters have been sampled every 60 seconds in each simulation. The period of sampling procedure is related to traffic loads. Shorter sampling periods can result in faster jamming detection, however, they can cause increased false positive rates especially on minor traffic loads. On the other hand, longer sampling periods can decrease false positive rates; the jamming detection period can get longer on the contrary. A random network topology has been created for each simulation and threshold levels of each parameter have been obtained from normal network behaviors during 36000 seconds period. Having obtained the threshold values, the simulation has been run further 36000 seconds to examine various jammer types. The simulations have been repeated five times minimum with five individual topologies and the average values of obtained results have been presented.

7. SIMULATION RESULTS

The detection rates and false positive rates are used to evaluate the performance of proposed advanced jamming detection algorithm, which has been presented in Section-5. The detection rates for various types of jammers with diverse rates of jammed nodes are shown in Figure-7, 8, and 9. The first crucial point in the figures is that although the detection rates appear to be very high, they have not reached to the level of 100%. The reason of this, the jamming detection procedure cannot be executed throughout six sampling periods in query cycles. The second critical point is that as the percentage of the jammed nodes increases, the detection rates increase as well. A decline in the number of boundary nodes particularly generates this situation. Another important fact is that higher detection rates can be achieved in case of bad connections (lossy connections, congested or faulty sensor nodes). The corruption rate of the QUERY-REPLY packets gets boosted and this occurrence affects the detection rate achievement in positive manner. The detection rates in scan and pulse jammer scenarios are generally lower than the others. This consequence is originated from the fact that they are not effective enough to occupy the communication channel completely and they attack to the sensor network at seldom intervals.

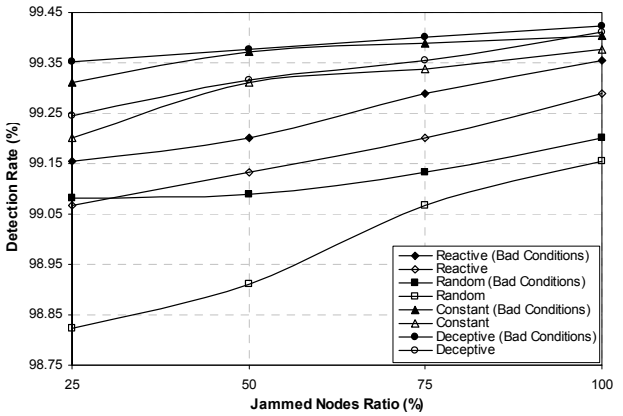

Figure-7. The detection rates of reactive, random, constant, and deceptive jammers in a range of scenarios.

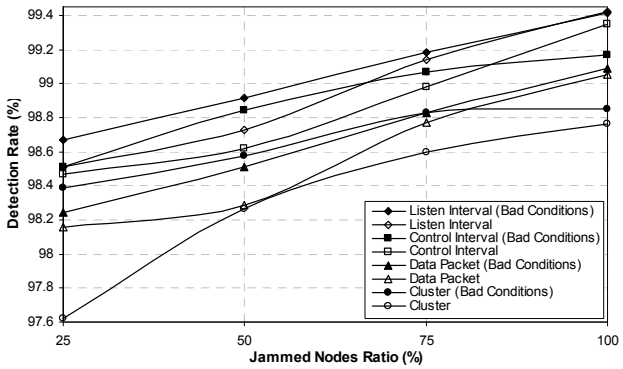

Figure-8. The detection rates of listen interval, control interval, data packet, and periodic cluster jammers in a range of scenarios.

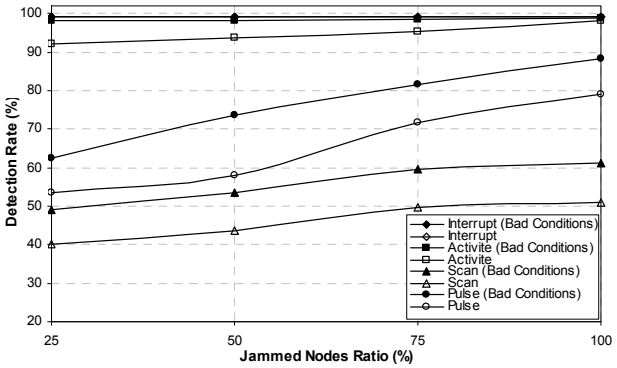

Figure-9. The detection rates of interrupt, activity, scan, and pulse jammers in a range of scenarios..

The false positive rates for various types of jammers with diverse rates of jammed nodes are shown in Figure-10, 11, 12. Notice that higher positive rates can be achieved compared to typical network conditions in bad connection situation. The motive behind this situation is to decrease the PDR level and to increase the BPR level on the contrary. In addition, the false positive rate may be boosted by faulty nodes in the sensor network. Another particular point is that while the coverage area broadens, the false positive rate decreases. As the number of directly jammed nodes increase, the number of nodes detecting false positive conditions decreases. If the Jammed Node Ratio (JNR) is zero, it means that there is no jammer in the network. Therefore, the false positive rates in three individual graphs are the same. The false positive rates, which are sampled at nonzero JNR values, can be accepted unreliable attack detections sampled from non jammed nodes.

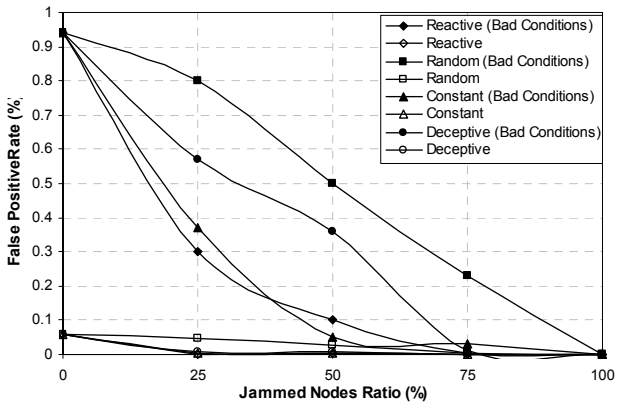

Figure-10. The false positive rates of reactive, random, constant, and deceptive jammers in a range of scenarios.

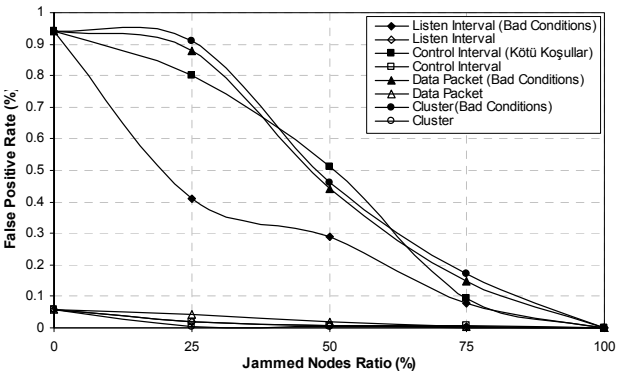

Figure-11. The false positive rates of listen interval, control interval, data packet, and periodic cluster jammers in a range of scenarios.

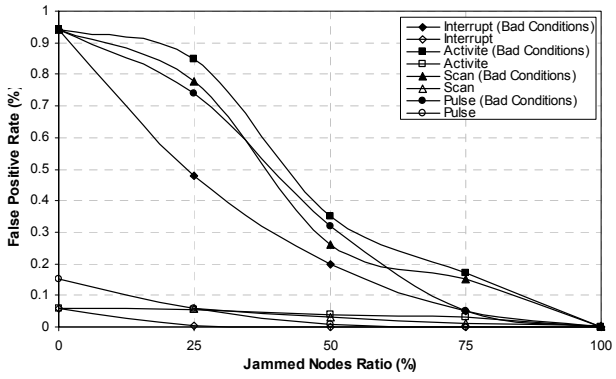

Figure-12. The false positive rates of interrupt, activity, scan, and pulse jammers in a range of scenarios

8. CONCLUSIONS

Jamming attacks are very serious of risk for wireless sensor nodes that can operate in very hostile environment with limited sources. To overcome the problems of the harsh environment, the nodes should apply efficient and successful policies for reliable and yet adaptive detection mechanisms. In this paper, we have proposed two jamming detection algorithms for many types of jammers. The proposed algorithms can separate network conditions caused by various types of jammers or caused by natural sources from each other along with high detection rate and low false positive rate. Another advantage is that no additional hardware is required to implement the algorithms on existing wireless sensor nodes. In the next study planned, the algorithms will be implemented on real wireless sensor nodes and, thus, the performance achievement of the algorithms in a real environment will be elaborated.

9. REFERENCES

[1] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam and E. Cayirci, "Wireless Sensor Networks: A Survey," Computer Networks, Vol. 38, No. 4, pp. 393-422, March 2002.

[2] Wei Ye, J. Heidemann, Deborah Estrin. "An energy-efficient MAC protocol for wireless sensor networks," IEEE Infocom, pages 1567–1576, NY, June 2002.

[3] A. Wood, J. Stankovic, and S. Son., "JAM: A jammed-area mapping service for sensor networks," In 24th IEEE Real-Time Systems Symposium, pages 286- 297, 2003.

[4] A.D.Wood and J.A.Stankovic, "Denial of service in sensor Networks", IEEE Computer, 35(10):54–62, Oct.2002.

[5] Yee Wei, L. Lodewijk, V. Hoesel, J. Doumen, P. Hartel, P.Havinga, "Energy-Efficient Link-Layer Jamming Attacks against Wireless Sensor Network MAC Protocols", SANS'05, November 7, 2005, Virginia, USA.

[6] W. Xu, W. Trappe, Y. Zhang, and T. Wood. "The feasibility of launching and detecting jamming attacks in wireless networks", In ACM MobiHoc '05, page to appear. ACM Press, 2005.

[7] J. Zhao and R. Govindan. "Understanding packet delivery performance in dense wireless sensor networks," In Proceedings of the First ACM SenSys, Nov. 2003.

[8] Y. Law, P. Hartel, J. den Hartog, and P. Havinga. "Link-layer jamming attacks on S-MAC," In 2nd European Workshop on Wireless Sensor Networks (EWSN 2005), pages 217–225. IEEE, 2005.

[9] www.omnetpp.org

[10] C. Hartung, J. Balasalle, and R. Han. "Node compromise in sensor networks: The need for secure systems"". Tech. Rep. Technical Report, CU-CS-988-04, Department of Computer Science, University of Colorado at Boulder, 2004.

[11] CrossBow Corporation, MICA2 Data Sheet [Online], http://www.xbow.com.MICA2 data sheet

[12] Anthony D. Wood, John A. Stankovic, and Gang Zhou, "DEEJAM: Defeating Energy-Efficient Jamming in IEEE 802.15.4-based Wireless Networks", SECON 2007, June 2007, San Diego, California, USA

[13] En-Yi A. Lin, Jan M. Rabaey, Adam Wolisz "Power-Efficient Rendez-vous Schemes for Dense Wireless Sensor Networks", In Proceedings of ICC 2004, Paris, France

[14] CC1000, Single Chip Very Low Power RF Transceiver Datasheet [online], Chipcon. http://focus.ti.com/lit/ds/symlink/cc1000.pdf