Hindawi
Security and Communication Networks
Volume 2017, Article ID 1531928, 9 pages
https://doi.org/10.1155/2017/1531928

Research Article

Practical Implementation of an Adaptive Detection-Defense Unit against Link Layer DoS Attacks for Wireless Sensor Networks

Murat Dener[1] and Omer Faruk Bay[2]

[1]*Graduate School of Natural and Applied Sciences, Gazi University, Besevler, Ankara, Turkey*
[2]*Department of Electronics and Computer, Gazi University, Besevler, Ankara, Turkey*

Correspondence should be addressed to Murat Dener; muratdener@gazi.edu.tr

Received 20 September 2016; Revised 6 December 2016; Accepted 14 December 2016; Published 15 January 2017

Academic Editor: Muhammad Khurram Khan

Wireless sensor networks (WSNs) have become a very popular subject in both industrial and academic fields of study due to the fact that they can operate on their own, do not require extra maintenance, and can be utilized in a wide variety of applications. In addition, the sensor nodes having limited hardware resources and power units cause certain security problems awaiting to be resolved. The Denial-of-Service (DoS) attacks, which cause disrupts in the communication of sensor nodes or abnormal situations, thus resulting in the decrease of the lifespan of the network, constitute a serious threat against the WSN security. Especially in military applications in which security is the most important design criterion, the WSN used in chemical and biological intrusion detection applications must be resistant against all forms of attacks. In this study, an adaptive detection-defense unit has been developed against the DoS attacks (packet collision, exhaustion, and unfairness) which occur in the data link layer. The developed unit has also been implemented on the TelosB nodes. Due to the new unit that was designed the lifespan of the nodes has been extended without the need for additional hardware by making them more secure against DoS attacks in the data link layer of the WSN.

1. Introduction

The WSN is exposed to a wide variety of security vulnerabilities due to the hardware limitations of the sensor nodes, wireless communication environment, real time processing needs, heterogenic structure, large number of nodes, need for measurability, mobility, the weight of the application environmental conditions, and cost [1]. Ensuring confidentiality, integrity, and availability, the primary goal of security is one of the most important problems to be solved in order to achieve time-critical and vital objectives [2]. When compared to the classical computer networks which are made up of personal or laptop computers that contain strong hardware and software nodes, the WSN displays many special characteristics [3]. Many of these unique features greatly make difficult the resolution of the security problem. One of the security requirements for WSNs is availability. Availability means being able to resume the services of the WSN even while under a Denial-of-Service (DoS) attack. DoS attacks are designed to interrupt services. It is a type of attack which causes the system being unable to provide services to anyone due to an individual constantly attacking the system or an attack aimed at using all the resources that belong to that system. There is no taking over, taking charge, or technically "hacking" involved. The main goal is to force the victim site to use up all its resources so that it cannot provide services to anyone. DoS attacks can occur in each protocol layer of the WSN and can render the victim nodes ineffective. In addition to the DoS attacks, the weight of excessive communication or calculation can cause the battery of the node to finish earlier than expected. Being unable to maintain the availability of the WSN may cause serious results. For example, in a military observation application, if a couple of nodes do not work properly, enemy units can infiltrate through this part of the WSN which is not working as it should. Ensuring the availability principle means that the protocol is resistant against DoS attacks. Packet collision attack [4], exhaustion attack [5], unfairness attack [6] can be given as examples of DoS attacks which occur in the data link layer. Not being able to prevent any one of these attacks makes that protocol

insecure. In this study, in order to establish the availability principle that is one of the WSN security requirements an Adaptive Detection and Defense Unit against packet collision, exhaustion, and unfairness attacks which occur in the data link layer has been developed and also implemented on the TelosB node. The second section describes related works. The third section describes the formation process of attacks. The fourth section defines the suggested unit and the fifth section further explains the adaptive system in the unit. The sixth section includes implementation practices; the seventh section provides experimental results from the study, and the last section presents the results of the study.

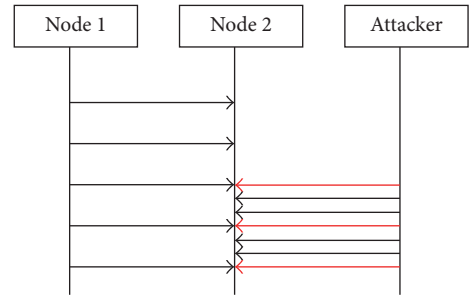

Figure 1: Packet collision and exhaustion attacks.

2. Related Works

The implementation of the suggested security protocols on the nodes is an important factor for the availability of the WSN. Therefore, it is important that the researchers increase their studies on the TinyOS operating system and the NesC programming language which are necessary to know in order for them to make applications on the nodes. When looking at the security solutions that are prevalent in the literature, only the TinySec [7], MiniSec [8], and SNEP [9] have software implementations on the sensor nodes. Even though the IEEE 802.15.4 [10] has been developed for the Wireless Personal Area Networks, it is also used in the WSN due to its low power exhaustion, low cost, and flexibility. These protocols are not able to provide the principle of availability which is one of the security needs of the WSN. In cases where the principle of availability is not provided, it means that this protocol is weak against DoS attacks.

TinySec supports two different security options: authenticated encryption (TinySec-AE) and authentication only (TinySec-Auth). With authenticated encryption, TinySec encrypts the data payload and authenticates the packet with a MAC. In authentication only mode, TinySec authenticates the entire packet with a MAC, but the data payload is not encrypted. TinySec provides data confidentiality, integrity, and authenticity with Skipjack + CBC-MAC. Minisec provides data confidentiality, integrity, and authenticity with Skipjack + OCB. SPINS have two security building blocks: SNEP and TESLA. SNEP provides semantic security, data authentication, replay protection, weak freshness, and low communication overhead. But, in these protocols there are no special tasks against link layer DoS attacks.

In addition, there are a couple of studies present in the literature which are aimed at preventing DoS attacks. These studies have not yet been implemented; only the simulations have been done. These are mapping protocols [11], FS-MAC [12], and G-MAC [13]. In mapping protocols several parameters are used to detect attacks. While under an attack and the enemy nodes occupy the area, it is very hard for a node to send a message. In order to overcome this situation, the jammed massages have been prioritized. The neighboring nodes receive the messages and prepare the lists of the jammed messages, thus allowing the designation of jammed areas. The FS-MAC has been created by adding a detection and defense unit to the IEEE 802.11 MAC protocol. The high number of packet collisions causes a packet collision attack, high number of RTS packets cause an exhaustion attack, and the waiting time causes an unfairness attack. A fuzzy logic has been used to designate the attack. The defensive method is that jammed nodes exposed to the attack wake up to sleep mode at short intervals until the attack ends. A central group method G-MAC is used against the DoS attacks. The nodes in the group use a gateway sensor to communicate with other nodes in the group. The packets obtained from other resources are neglected, thus allowing for avoidance from deceptive jammer attacks. In another study [14] that was conducted by Xu et al., four types of attack were designated and certain methods were developed to identify them. The first method is related to the signal strength, because during an attack there can be abnormal changes in the signal strength. The second method is the Carrier sense intervals. The Carrier sense intervals are widened during an attack. The other method is to control packet arrival rates. Of course these values are not enough by themselves. Without the presence of an attack on existing nodes in the network, under certain conditions, these ratios may show abnormal changes.

3. Formation of Attacks

This section describes formation of packet collision, exhaustion, and unfairness attacks. Figure 1 illustrates how packet collision and exhaustion attacks occur.

Node 1 sends a message to Node 2 after performing the detection operation in the environment. Since the CSMA is canceled at the attacking node, it continuously sends a message to Node 2 without waiting for the media to be empty. As a result a packet collision and exhaustion attack occur [15]. Packet collision attack occurs when the attacker node sends a message to the node in the environment once. In the event that the message sent by the attacker node is constant, exhaustion attack occurs.

Figure 2 shows how unfairness attack occurs.

Node 1 sends a message to Node 2 after performing the detection operation in the environment. Attacker node keeps Node 2 busy by sending a message. As a result a unfairness attack occurs [16]. In the CSMA based Medium Access Protocols, every node has the same amount of time for using up the media. Every node makes an effort to take over media and this is fairly distributed. The attacking node sends packets to the network by taking advantage of this rule. By doing this, instead of the nodes belonging to the channel using up the media, these attacking nodes take over.

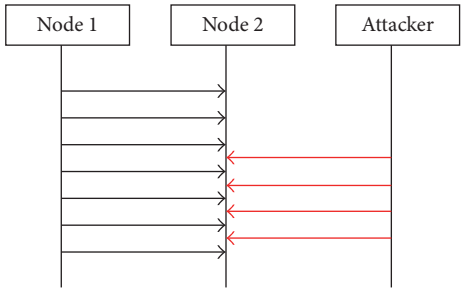

Figure 2: Unfairness attack.

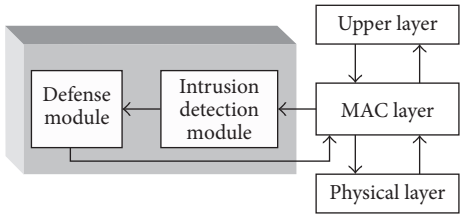

Figure 3: Structure of our proposed unit.

4. Proposed Method

This section describes the suggested adaptive detection-defense unit for packet collision, exhaustion, and unfairness attacks. Figure 3 shows the structure of our proposed unit. We improve the security of MAC layer through adding two special modules, intrusion detection module and intrusion defense module, into the original TinyOS operating system.

Detection module determines whether the intrusion exists or not. Then, if attacks are found, defense module is activated.

4.1. Packet Collision and Exhaustion Attack. The flowchart of the Adaptive Detection and Defense Unit that has been developed against the packet collision and exhaustion attacks is demonstrated in Figure 4.

The nodes in the environment send data, with a 0x11 message type, to the cluster head or base station every 60 ms. When this time period reaches 1 minute (60000 ms) the node attaches how many packets it has sent to the message packet and sends them through a 0x22 message type. The cluster head and base station which receives this message can determine to which node this packet belongs to. Then, it finds the number of packets received from this node. If there is no difference between the number of packets sent by that node and the number of packets received, it means that the network is operating in a healthy manner. If the packet disappeared during transfer, it means that a packet collision has occurred. Under normal circumstances, the average rate of packet delivery is very high with no attacks. The decreased rate of packet delivery lower than threshold value facilitates identifying attack scenarios for any types of attackers responsible for DoS attacks.

The cluster head or base station which detects this problem sends a warning message to that node and the node which receives this message decreases its message sending frequency and continues to send messages. However, energy of the attacker node decreased or exhausted after a set period of time has been taken into consideration. To prevent the network from slow data transmission in this process, head of the clusters or base station transmits a message to enable the node to transmit data like previous time intervals if no packets are lost in a given time. This time interval will be decided by the adaptive system which is described in the next section.

As known within the literature [17], the Rate Limiting Technique is used for kinds of this attack. Rate Limiting Technique is demonstrated in Figure 5.

As can be seen in Figure 3, the amount of time in which the radio is active has been reduced. If the communication times of friendly nodes and the attacking times of attacker nodes do not overlap, the attacker will no longer be effective. One of the ways to reduce this possibility is to reduce the listening periods of the nodes. In other words, it is to sleep for a longer period of time during a listening/sleeping period and to be able to communicate in a shorter time. As a result the possibility of the attacker to make the attacking packets overlap with the communication times of the nodes is lowered. Due to this technique, the lifespan of the network increases considerably. By reducing the amount of data that is received and kept by the radio, the impact of the attack is reduced.

4.2. Unfairness Attack. The flowchart of the Adaptive Detection and Defense Unit that has been developed against the unfairness attack is demonstrated in Figure 6.

In the CSMA based Common Access Protocols, every node has the same amount of time for using up the media. For example, if five nodes will send data to the cluster head or base station, each one will be taking up % 20 of the media. Utilization rate of media = (the number of packets sent by x node/the total number of packets sent by the nodes) $*$ 100. As can be seen by the formula above, every node will send an equal number of packets to the cluster head or base station (for example, 50) and according to the formula;

$$\text{Utilization rate of media} = \left(\frac{50}{50} + 50 + 50 + 50 + 50\right) * 100 = \left(\frac{50}{250}\right) * 100 = 20. \quad (1)$$

In other words, since the cluster head or base station is aware of the number of nodes that is in interaction with, it is able to calculate their rate of media usage while the nodes are sending messages every 1000 ms. If this rate is equal to that which is calculated by the cluster head or base station, it means that the network is operating in a healthy manner. However, if this value is below what it should be, it means that the media are being used by an attacker node. The cluster head or base stations which detect this problem send a message to the node and that node continues its message transmission by reducing the size of the packets. Size of the packets is decided by the adaptive system which is described in the next section. The small sized packets when compared to large size packets need lower transmission powers. The possibility of an error

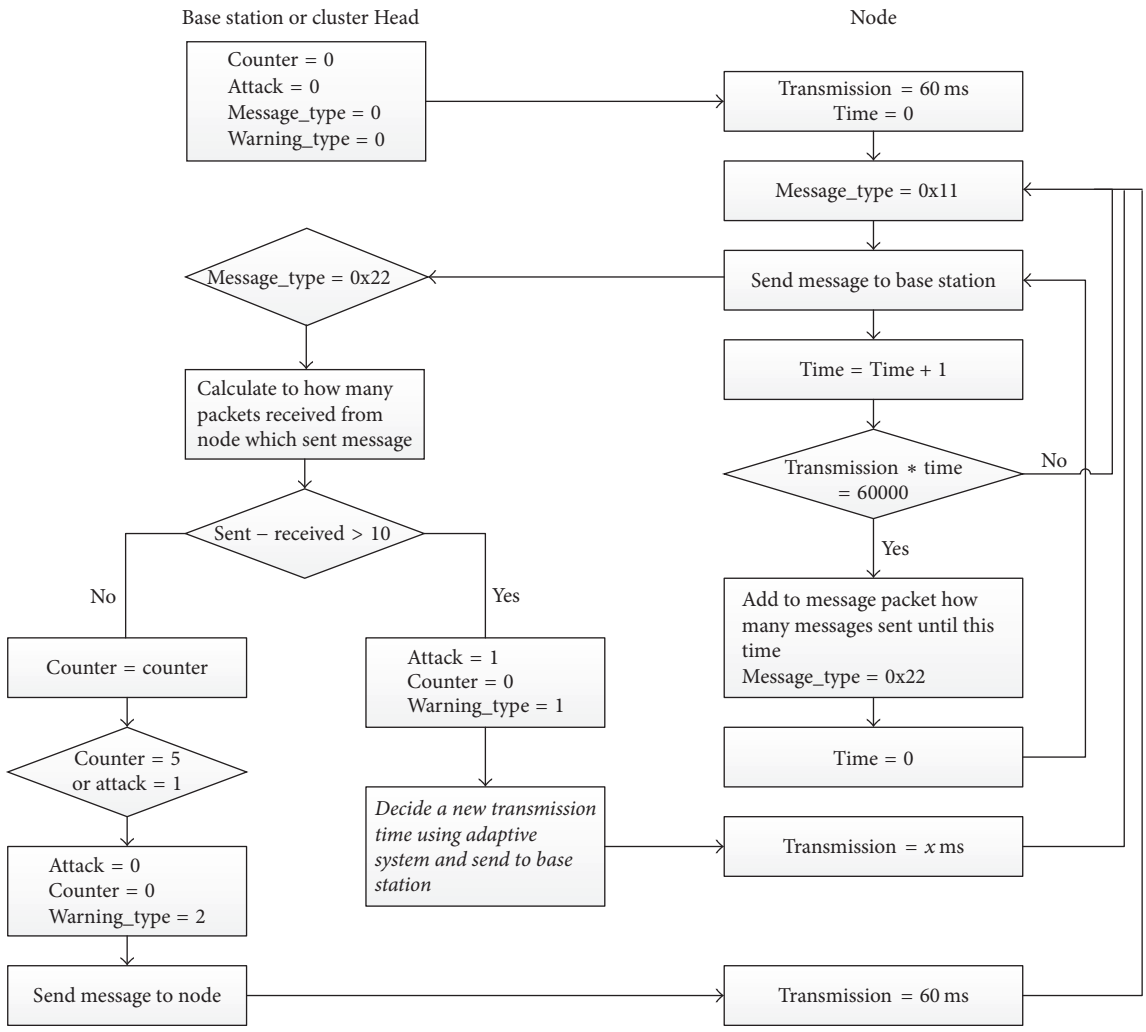

Figure 4: Flowchart of adaptive detection-defense unit for packet collision and exhaustion attacks.

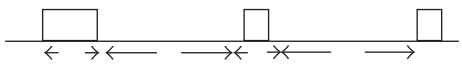

Figure 5: Rate Limiting Technique.

occurring is quite low when compared to larger size packets. Due to the small sized packets, the nodes that belong to the network are able to increase the amount of time in which they will use the media. Once the cluster head or the base station determines that the attack is over, a message is sent to the nodes allowing them to return to their previous message sending types.

5. Adaptive System

This section describes adaptive system in detection and defense unit.

5.1. Packet Collision and Exhaustion Attack. The nodes initially transmit the packet of messages every 60 ms to detect packet collision and exhaustion attacks. It is necessary to increase 60 ms in order to limit the speed at the moment of attack.

The developed adaptive system will decide the extent of increase. The system successfully computes the packet rate by increasing the transmission period every minute. This process is maintained as long as the successfully transmitted packet rate is increased. The process is finished whenever this rate is lower than the previous rate. Figure 7 illustrates the flowchart of how adaptive system reacts to packet collision and exhaustion attacks.

Table 1 shows an example of results from system operation during packet collision and exhaustion attacks.

As seen in Table 1, adaptive system computes the successfully transmitted packet rate, at the end of each minute during an attack. The frequency of packet transmission is adjusted to 1000 ms when this rate is detected to be 1000 ms maximum. While normally 997 packets are delivered, the fact that during an attack this number is being reduced to 60 packets can be explained by the following. When the attack occurs, the main objective is to reduce the number of packets lost. There are

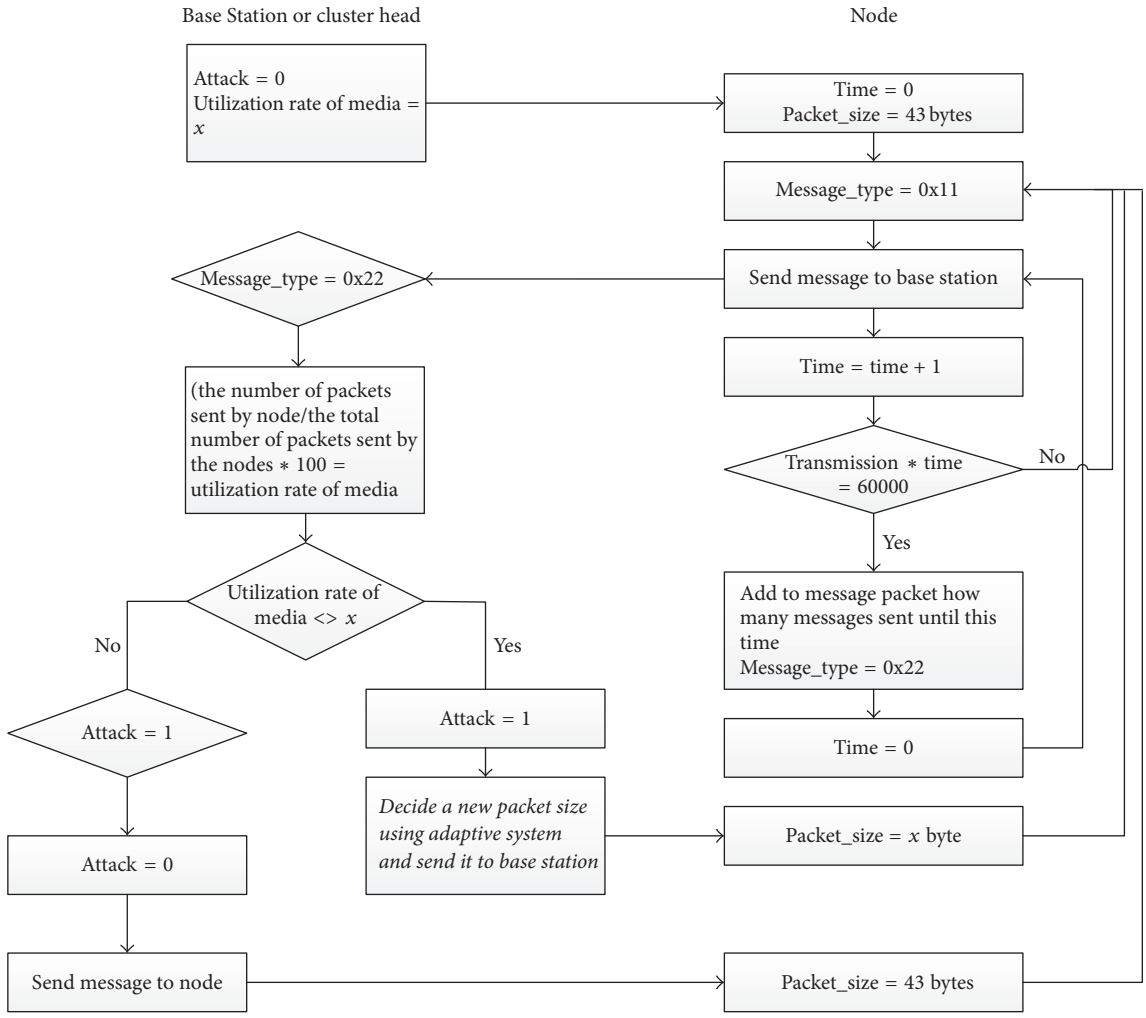

Figure 6: Flowchart of adaptive detection-defense unit for unfairness attack.

already samples from the 60 packets sent in 1 minute during an attack and the 997 packets that are normally delivered. Therefore, it is more efficient to use the value which allowed for the successful delivery of the most amount of packets when an attack took place.

5.2. Unfairness Attack. The nodes initially transmit message packets at 43 bytes. The size of message packet needs to be reduced during an attack. It is adaptive system that decides to what extent it should be reduced. The system computes the usage rate of medium by reducing the size of the packet each minute. This process carries on as long as use rate of medium is increased. The process is finished whenever this rate is equal to or less than the previous rate. Figure 8 illustrates the flowchart of how adaptive system reacts to an unfairness attack.

Table 2 shows an example of results from system operation during unfairness attacks.

As seen in the Table 2, adaptive system computes the usage rate of medium at the end of each minute during an attack. The size of the packet is adjusted to 19 bytes when this rate is detected to be 19 bytes maximum. Adaptive system decides the value that needs to be used in order to increase the successfully transmitted packet rate and the usage rate of medium during attacks. The system is engaged in comparison for a certain period of time and then determines the values to be used at the end of this period. The developed adaptive detect-defense unit is resistant to the types of DoS attackers (constant jammer, deceptive jammer, reactive jammer, and random jammer) because of the operating form of the system.

6. Implementation

The architecture of the implemented application is given in Figure 9.

When you plug the TelosB node into the usb port of the computer, it acts as a base station. The sensor nodes in the medium transmit the data sensed to the base station. When base station receives a packet over the radio, it transmits it to the serial port of the computer. In Cygwin environment, the following encodings are used to transfer the sensed data to the PC via the serial port. With these codes, the Listen.java file, which is inside the TinyOS folder, runs.

```
cd tools/java
```

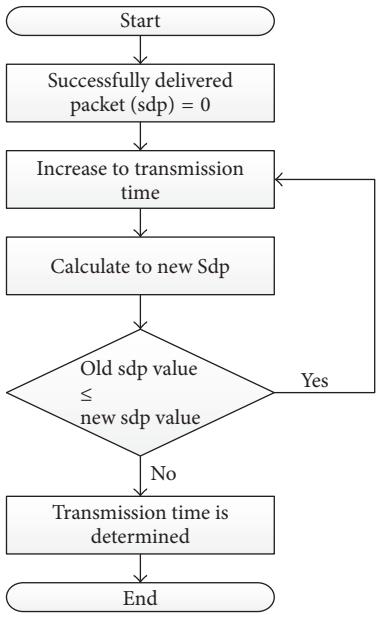

Figure 7: Flowchart of adaptive system for packet collision and exhaustion attacks.

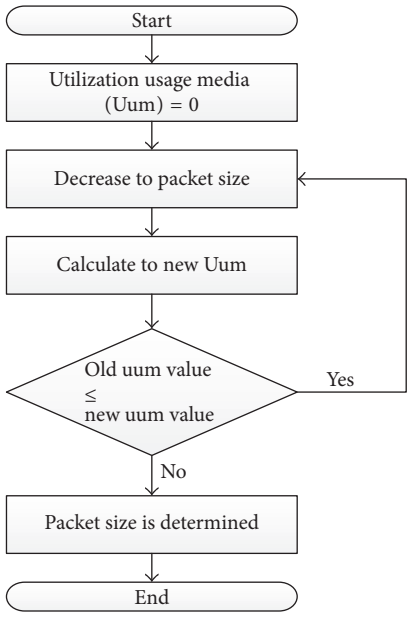

Figure 8: Flowchart of adaptive system for unfairness attack.

make

export MOTECOM=serial@COM3:telos

java net.tinyos.tools.Listen

In order to see the results, additions have been made to the Listen. java program within the TinyOS folder which enables the data received by the serial port to be transmitted to the computer. Through these additions, the data that comes to the serial port are inserted into the database. There are two

Table 1: Successfully delivered packets during an attack.

During an attack (ms)	Average delivered packets	Average packets lost	Successfully delivered packets (%)
60	997	120	87.96
80	749	90	87.98
100	558	65	88.35
120	497	57	88.53
150	398	36	90.95
200	298	26	91.28
250	237	20	91.56
300	199	14	92.96
400	148	10	93.24
500	118	7	94.07
600	100	5	95.00
750	79	3	96.20
800	74	2	97.30
1000	60	1	98.33
1200	50	1	98.00

Table 2: Utilization rate of media during an attack.

Packet size	Utilization rate of media (%)
43	53
41	56
37	60
33	65
29	69
27	70
25	74
22	77
19	80
17	80

important points in the additions. One of them is database connection and the other is query. Codes are given below.

```
Connection database=DriverManager.
getConnection("jdbc:" + "postgresql:
//localhost:5432/
postgres","postgres", "postgres");
Statement query=database.
createStatement();
query.executeUpdate("insert into table
(data,counter)values('"+data+"',
'"+counter+"')");
```

The following link can be used to access the Listen.java program:

http://w3.gazi.edu.tr/~muratdener/Listen_java.pdf

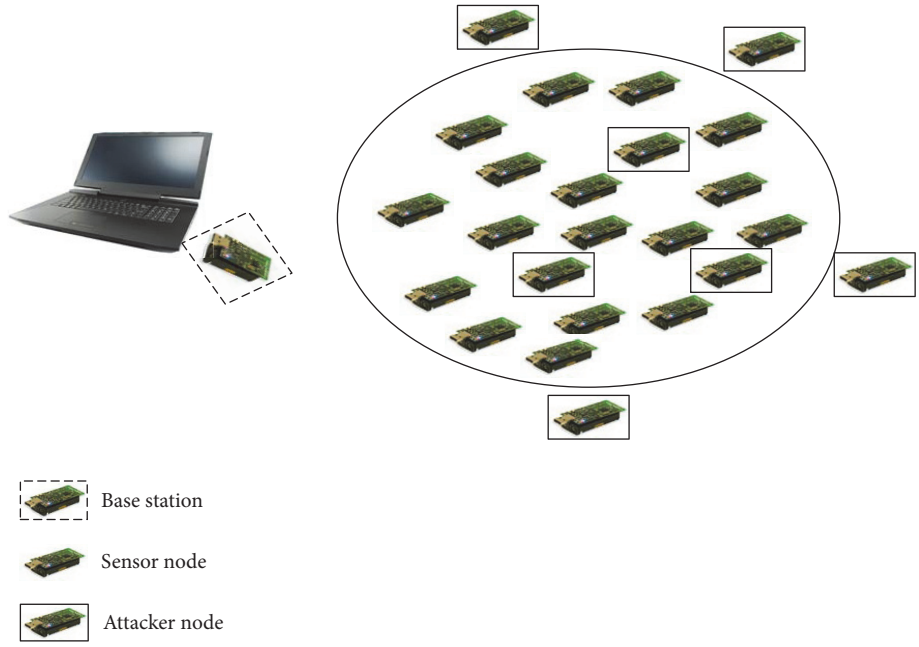

Figure 9: Architecture of the implemented application.

PostgreSQL has been used for the management of the database system. An interface has been written by using the Delphi program in order to see the results while looking at the data saved in the database. A total of 600 lines of NesC code were written in the present study during formation of attack nodes and adaptive detect-defense unit. There are 3 different code files available. These are for base station, sensor nodes, and attacker nodes. The base station and the sensor nodes operate according to Figures 4 and 6.

In attacker nodes, CSMA is deactivated to create packet collision and exhaustion attacks. The code that transmitted data to the medium with small packets is installed on the attacker node. In addition, the code that transmitted data to the medium with normal packets is installed on the attacker node to create unfairness attack. Attacker nodes operate according to Figures 1 and 2.

The following links can be used to access the NesC files of base station, sensor nodes, and attacker nodes.

http://w3.gazi.edu.tr/~muratdener/Base_Station.pdf

http://w3.gazi.edu.tr/~muratdener/Sensor_Node.pdf

http://w3.gazi.edu.tr/~muratdener/Attacker_Node.pdf

7. Experimental Results

To test our scheme we used TOSSIM—the simulator for TinyOS. It compiles directly from TinyOS code. Deriving the simulation from the same code that runs on real hardware greatly simplifies the development process. TOSSIM supports several realistic radiopropagation models and has been validated against real deployments for several applications. TOSSIM also incorporates TinyViz, a Javabased graphic user interface (GUI), that allows for visualization and control of the simulation as it runs, inspecting debug messages, radio and UART packets, and so forth.

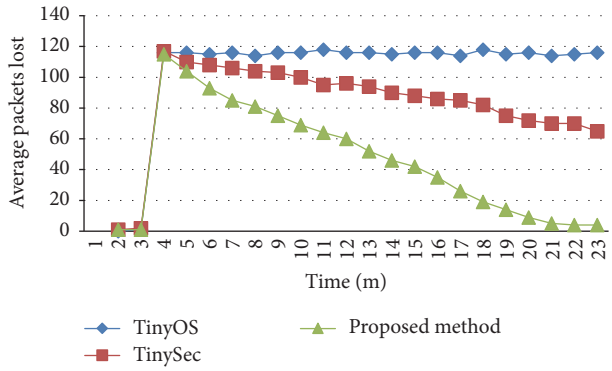

Figure 10: Results for packet collision and exhaustion attacks.

100 nodes are used as a network node; the base station is fixed. Each node is placed randomly within a 100 × 100 cell. Comparative performance analysis results are presented based on average packets lost and utilization rate of media themes. Average results are obtained under intense communication of network by running simulation 10 times.

(a) Figure 10 shows the comparative results of the proposed method, available TinyOS system, and TinySec protocol during packet collision and exhaustion attacks.

The loss of packets was 0 because no attacks occurred during the first 2 minutes. The attacker nodes began attacking between minute 2 and minute 3 and the 120 packets on average were lost. The developed adaptive detection and defense unit detected the attack after minute 3. The node that limited its rate upon receiving warning message of base station reduced its rate to minimize loss of packets

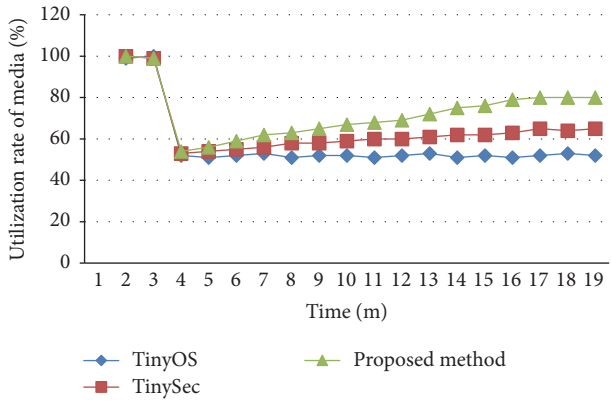

Figure 11: Results for unfairness attack.

for next periods. In TinySec protocol, because there is no special unit against collision and exhaustion attacks, it did not obtain same success with our proposed method. But, TinySec has other security solutions in its own protocol; this is reduced to average packet lost values. However, average loss of packets continues in TinyOS because TinyOS system does not provide the principle of availability. TinyOS system is still under attack and the frequency of packet transmission remains the same.

(b) Figure 11 shows the comparative results of the proposed method, available TinyOS system, and TinySec protocol during an unfairness attack.

The usage rate of the medium was 100% as no attacks occurred during the first 2 minutes. The attacker node began attacking between minute 2 and minute 3 and the use rate of the medium decreased to 50%. The developed adaptive detection and defense unit detected the attack after minute 3. The usage rate of the medium increased to 80% after the nodes received the warning message to reduce the size of packets. In TinySec protocol, because there is no special unit against unfairness attack, it did not obtain same success with our proposed method. But, TinySec has other security solutions in its own protocol; this is increased to utilization rate of media values. However, the usage rate of the medium remained at 53% in TinyOS because the size of the packets remained the same on TinyOS system that did not provide the principle of availability and the attack was carried on.

8. Conclusions

All security requirements must be provided because wireless sensor networks are used in very important applications such as military applications and health applications. Additionally, the sensor nodes having limited hardware resources and power units cause security vulnerabilities which await a resolution. It is therefore required to develop security protocols to fully cover such security threats.

Even if all of other conditions are provided, if the principle of availability which is one of the security needs of the WSN is not provided, the WSN will be defenseless against DoS attacks. This means that the WSN will not be able to perform its tasks during a packet collision, exhaustion, and unfairness attacks. As known, if the principle of availability has not been established in the security application that is developed, the network will not be able to perform its tasks and stop working during DoS attacks. Even through the DoS attacks do not change the contents of the data in the network, the WSN that is victim to the attack will become disabled. The energy exhaustion of the nodes that constitute the WSN as well as the processor cycle increases. Due to this the lifespan of the network is reduced. As a result, security requirements need to be provided. In this study, an Adaptive Detection and Defense Unit against the packet collision, exhaustion, and unfairness attacks that occur in the data link layer have been carried out in order to provide the WSN security need of principle of availability.

Comparative performance analysis results are obtained in TOSSIM simulation platform based on average packets lost and utilization rate of media themes. Proposed method has better results than TinyOS system and TinySec protocol. Although TinySec is security protocol which provides data confidentially, integrity, and authentication, because it has no specific unit against link layer DoS attack, it did not show same success when compared to our method.

The developed unit is also implemented on the TelosB nodes. Due to the designed adaptive detection-defense unit, the lifespan of the nodes has been extended without the need for any further hardware by making the wireless sensor networks more secure against the DoS attacks that occur in the data link layer.

Competing Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

References

[1] E. Sharifi, M. Khandan, and M. Shamsi, "MAC protocols security in wireless sensor networks: a survey," *International Journal of Computer and Information Technology*, vol. 3, no. 1, pp. 105–109, 2014.

[2] G. Mahalakshmi and P. Subathra, "A survey on prevention approaches for denial of sleep attacks in wireless networks," *Journal of Emerging Technologies in Web Intelligence*, vol. 6, no. 1, pp. 106–110, 2014.

[3] P. Kour and L. C. Panwar, "A review on security challenges and attacks in wireless sensor networks," *International Journal of Science and Research*, vol. 3, no. 5, pp. 1360–1364, 2014.

[4] H. Ali, A. A. Mamun, and S. Anwar, "All possible security concern and solutions of WSN: a comprehensive study," *International Journal of Computer Science and Technology*, vol. 6, no. 4, pp. 64–74, 2015.

[5] D. Singla and C. Diwaker, "Analysis of security attacks in wireless sensor networks," *International Journal of Software and Web Sciences*, vol. 14, pp. 26–30, 2014.

[6] S. Ghildiyal, A. K. Mishra, A. Gupta, and N. Garg, "Analysis of Denial of Service (DOS) Attacks in wireless sensor networks," *International Journal of Research in Engineering and Technology*, vol. 3, no. 22, pp. 140–143, 2014.

[7] C. Karlof, N. Sastry, and D. Wagner, "TinySEC: a link layer security architecture for wireless sensor networks," in *Proceedings of the 2nd ACM Conference on Embedded Networked Sensor Systems (SENSYS '04)*, pp. 162–175, Baltimore, Md, USA, November 2004.

[8] M. Luk, G. Mezzour, A. Perrig, and V. Gligor, "MiniSec: a secure sensor network communication architecture," in *Proceedings of the 6th International Symposium on Information Processing in Sensor Networks (IPSN '07)*, pp. 479–488, Cambridge, Massachusetts, USA, April 2007.

[9] A. Perrig, R. Szewczyk, J. D. Tygar, V. Wen, and D. E. Culler, "SPINS: security protocols for sensor networks," *Wireless Networks*, vol. 8, no. 5, pp. 521–534, 2002.

[10] IEEE-TG15.4, *Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (LR-WPANs)*, IEEE Standard for Information Technology, 2003.

[11] A. Wood, J. Stankovic, and S. Son, "JAM: a jammed-area mapping service for sensor networks," in *Proceedings of the 24th IEEE Real-Time Systems Symposium (RTSS '03)*, pp. 286–297, Cancun, Mexico, December 2003.

[12] Q. Ren and Q. Liang, "Fuzzy logic-optimized secure media access control (FSMAC) protocol," in *Proceedings of the IEEE International Conference on Computational Intelligence for Homeland Security and Personal Safety (CIHSPS '05)*, pp. 37–43, April 2005.

[13] M. Brownfield, Y. Gupta, and N. Davis, "Wireless sensor network denial of sleep attack," in *Proceedings of the 6th Annual IEEE SMC Information Assurance Workshop (IAW '05)*, pp. 356–364, West Point, NY, USA, June 2005.

[14] W. Xu, W. Trappe, Y. Zhang, and T. Wood, "The feasibility of launching and detecting jamming attacks in wireless networks," in *Proceedings of the 6th ACM International Symposium on Mobile Ad Hoc Networking and Computing (MOBIHOC '05)*, pp. 46–57, Chicago, Ill, USA, May 2005.

[15] K. A. Basith and C. Balarengadurai, "Detection of DDoS attacks in IEEE 802.15.4—a review," *International Journal of Modern Sciences and Engineering Technology*, vol. 2, no. 6, pp. 103–111, 2015.

[16] S. Biswas and S. Adhikari, "A survey of security attacks, defenses and security mechanisms in wireless sensor network," *International Journal of Computer Applications*, vol. 131, no. 17, pp. 28–35, 2015.

[17] M. Panda, "Security threats at each layer of wireless sensor networks," *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 3, no. 11, pp. 61–67, 2013.