Detection Algorithm for Sinkhole Attack in Body Area Sensor Networks Using Local Information

Adnan Nadeem and Turki Alghamdi
(Corresponding author: Adnan Nadeem)

Faculty of Computer, Information System, Islamic University of Madinah
Madinah, Saudi Arabia
(Email: adnan.nadeem@iu.edu.sa)

(Received Jan. 20, 2018; Revised and Accepted Apr. 28, 2018; First Online Jan. 11, 2019)

Abstract

Wireless Body Area Sensors Networks (BAN) have emerged as new applied wireless networking technology with the development of wearable and implanted sensors. BAN has novel application in healthcare, sports, human activity monitoring, disability assistance and entertainment. BAN is now using for real time monitoring and assistance of the patients. BAN operations are vulnerable to various security attacks, including basic and advance attacks. In this paper, we introduce and illustrate the sinkhole attack in a BAN. Then we propose our sinkhole detection algorithm that utilizes the information from data aggregation algorithm to detect a sink hole attacker. Finally, we analyze the performance of the BAN in terms of throughput, latency and packet breakdown and the performance of our detection algorithm. Simulation results show that this attack could severely degrade (up to 40%) the overall performance of the network. The propose detection algorithm has good performance in terms of high success (85% on average) and low (6% on average) false alarm rates.

Keywords: Body Area Networking Technology; Performance Analysis of BAN; Security & Privacy; Sinkhole Attack

1 Introduction

Wireless Body Area Sensor Networks (BANs) is an emerging wireless networking technology. It consist of wearable sensors with the capability of monitoring physiological parameters of the body *e.g.* ECG, temperature, heart rate, EMG and blood pressure measurements [4, 19]. BAN has its applications in health-care, fitness, sports and entertainment. Beside these major applications some novel applications areas of BAN has also emerged recently. BAN consists of wearable or implanted sensors, data aggregator and a gateway device called sink, where all the sense information is aggregated for analysis and decision making. All the data sense by the sensors must be routed to the gateway device. However, this process of data aggregation and routing is vulnerable to various attacks. Specifically in health care applications of BAN where it use to monitor and assists patients health the presence of malicious node could be life threatening [6, 18].

Security & Privacy is one of the major concerns for the researchers involve in BAN along with energy efficient operations. Considering the healthcare applications of BAN, security and privacy of information communicated over the network become highly important. BAN like other networks is also vulnerable to a range of security attacks [11] that could seriously degrade the performance of the network. Sink hole attack is one of them, in this the attacker gets attach with the network claiming to be a sink node and causes both security and privacy issues. Therefore, in this paper we first illustrate the sink hole attack in BAN and then propose out sink hole detection algorithm that utilizes the audit data from the data aggregation techniques to detect sinkhole attack. We analyze the affect of this attack on BAN performance and the performance of our sink hole detection algorithm using a simulation based case study.

The rest of the paper is organized as follows: Section 2 presents the overview and classification of security attacks in a BAN. Section 3, we present the illustration of sinkhole attack. In Section 4, we briefly review the related work. Then we present our proposed sink hole detection algorithm in Section 5. In Section 6, we present the performance analysis of BAN under sinkhole attack and the performance of its detection algorithm, including the simulation results. Finally, we summarize our work and highlight possible future work in Section 7.

2 Security Attacks in BAN

Similar to wireless sensor network (WSN), BAN is also vulnerable to various attacks. Authors in [2] have defined the threats and their security requirements in BAN. Table 1 illustrates the threats and the related security requirements. It mainly discusses the classical basic security requirements including integrity, confidentiality, authentication, availability which exists in almost all data communication networks.

Table 1: Threats and related security requirements in BAN [2]

Threats	Security Requirements
Data Modification	Integrity
Impersonation	Authentication
Eavesdropping	Confidentiality
Replying	Integrity
DoS	Availability

We classify security attacks in BAN as either basic and advance attacks. Basic attacks include all the attacks with traditional security attributes/ requirements. Whereas advance attack we include the specialized attack that could be launch in BAN by the attacker to achieve the certain goal. Figure 1 presents our classification of attacks in BAN. Attacks in basic attack category has been extensively discussed in the literature therefore, we will only discuss the advance attacks.

2.1 Data Freshness

Decisions made by physicians or health caregivers are mainly dependent on the freshness of data. Therefore, replaying old messages in WBAN could cause serious consequences.

2.2 Reliability

Due to the type of sensors and its energy constraints, operations reliability of nodes and operations in BAN is a major issue. The BAN applications have several Reliability [9] & Quality of Service [13] problems. Considering the health care applications of BAN this issue could be significant. In emergency situations, if the data is not communicated within the specified time period then it can incur serious consequences even a loss of life. Devices implanted inside the human body are prone to absorption and attenuation because of material composition and structure of the human body.

2.3 Trust Management

Energy restrictions make the key distribution between the nodes a major challenge. Public key cryptography, which is majorly used in Digital signatures for key exchange consumes much more energy than Symmetric cryptography. Therefore, authors in [15] propose static node deployment for energy efficient operations. Considering the energy Moreover, as per the new observation, same physiological values monitored from different parts of the body within the same time frame, exhibit similar characteristics, which can put the Trust management procedure on stake.

2.4 Privacy

Several aspects of the Privacy and social issues exist in WBANs. Health records can be stolen upon by the emergency technician in case of emergency for monetary gains. This issue arrives when extra privilege to information is granted, thus leading to theft of data private to the patient. This may include name, social security number, mailing address, medical record history, *etc.* Also, people might not want some data to be made public *e.g.* early stage pregnancy. Below are the attacks which deal with privacy.

2.4.1 Monitoring and Eavesdropping

Monitoring and eavesdropping is an attack for privacy. The attacker can easily gather the data by snooping.

2.4.2 Traffic Analysis

The attacker can read and understand the communication between two parties by getting traffic patterns and can be harmful to legitimate users.

2.4.3 Camouflage Adversaries

An attacker can introduce a new node or tries to compromise the other nodes by hiding it in the sensor network. Sensor nodes pretend themselves as a common network node in order to capture the packets.

2.4.4 Privacy

Privacy issue also exists on the storage server/site as the site is aware of the ownership of records *i.e.*, which record belongs to which patient. Moreover link ability of records can help stealing vast amount of data linked among one another. Furthermore, Location privacy breach can expose the knowledge of patient?s whereabouts and location, calculated by exploiting the capability of the sensors installed. Privacy has a strong association with the security aspects of Access control and Authorization [10]. Biological signals collected from ECG and EEG can reveal information of psychological status and identity of the subject, which can reveal emotion assessment and thus raise privacy concerns [1].

2.4.5 Sinkhole Attack

A sinkhole is a denial of service attack well defined and extensively research in WSN. In this paper, we first describe and illustrate this attack in a BAN. We have considered multi hop scenario of BAN where a malicious node falsely announces itself as a sink node. The entire sensor node sends their information to this node which drops all the information [12]. There are various techniques have been proposed to detect attacks in wireless sensor network some of them using cryptographic techniques such as [3,16,20], however, few researchers have focus on investigating it in body area network. We believe this attack

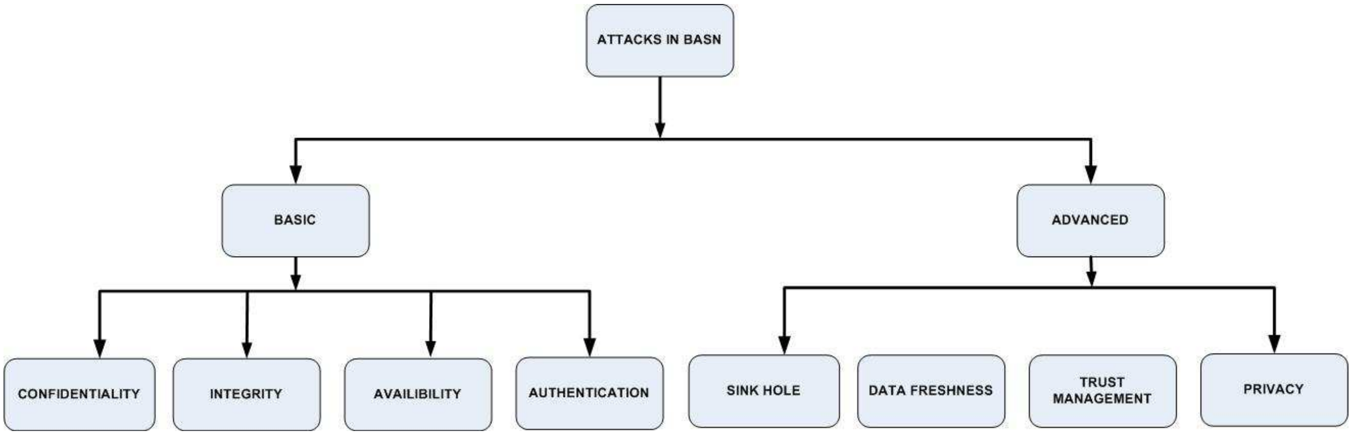

Figure 1: Security attacks in BAN

could seriously degrade the performance of the body area network. This motivates us to analyze the effect of sinkhole attacks on the performance of BAN in this paper.

3 Illustration of Sinkhole Attack in BAN

The sinkhole attack is one of the severe attacks that prevents the legible sink or gateway node in receiving complete and correct information, and creates a severe threat to applications. In a Sinkhole attack [12,14]; A malicious node tries to capture whole traffic from network, by impersonating itself as a sink node in the network. As a result, the attacker gets all traffic that is to be transmitted to legitimate sink node. In this way it can then introduce various severe types of attacks, like selective forwarding, modifying or even dropping the packets coming through.

Wireless body area sensor network plays important role in health-care applications from basic patient monitoring to the specific disease monitoring and detection. Third generation of sensors kits such as ECG and EMG kits are available to use in various healthcare tasks. We assume third generation wearable sensors such as temperature, blood pressure, ECG. The model which we have used is shown in Figure 2. There are six nodes and their placement is as follows.

Table 2: Placement of nodes on the Human body

Node	Placement
0	Right Hip (Sink)
1	Left Arm
2	Right Arm
3	Left Ankle
4	Right Ankle
5	Chest
6	Right Hip

We now consider the network in Figure 2 and illustrate how an attacker can launch sinkhole attack. This network consists of five sensors and a sink node. The nodes in the network operate in a multi hop scenario.

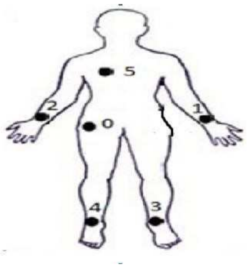

Figure 2: Show the model of BAN

Figure 3 shows the scenario of normal nodes with green lines connected with each other wirelessly and they operate normally. The green boxes show the normal packet flow between the sink node and the other nodes in the network. Figure 4 shows a scenario where an attacker gets connected with the network. This node which is not an authorized node can act as a sink hole and affects the performance of the network. The malicious node after being the part of network tries to capture network traffic by announcing himself as a sink to all nodes. This is done through sending a false message as shown in Figure 5.

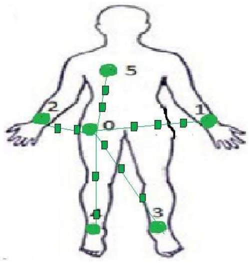

Figure 3: Show the scenario with normal operations of BAN

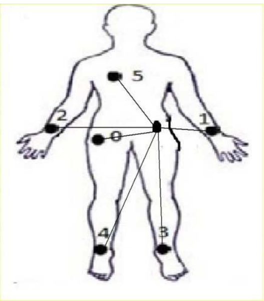

Figure 4: Shows the scenario with an attacker connected to a network

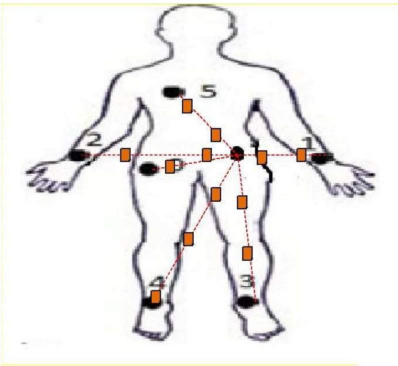

Figure 5: Attacker falsely announcing himself as sink node

When data reaches this malicious sink node, then instead of forwarding the packets to the actual sink it drops the packets as shown in Figure 6. This behavior of attacker prevents data traffic from reaching the legitimate sink node. This could seriously degrade the performance of the network. In this paper we have perform an analysis of the degree of impact that this attack can have on the performance of the network and parameters on which the level of performance degradation depends.

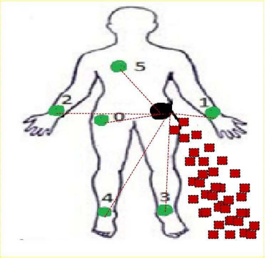

Figure 6: Shows packets dropped by attacker node

4 Related Work

Security and privacy is one of the prime concerns in the BAN research [12,14]. Several studies have suggested different type of detection algorithms in wireless sensor networks with regard to sinkhole attack. The sinkhole attack normally occurs where; there is symmetric traffic among the sensor nodes [14]. Sinkhole attack is devastating because of the weak computation and battery power of the sensor nodes in these networks.

Karlof [8]propose a trust scheme to the routing protocol for detection of sinkhole and wormhole attacks in a sensor network; however activity of nodes in a loose mode is essential. It has been shown that packet restriction can disclose the limit of transfer time and each packet?s distance. It has been suggested that strong authentication mechanism should be used to avoid such types of attacks in wireless sensor networks [12,14].

Authors in [4,12,14] first suggest a way to detect sinkhole attacks in which the BS in the detection process, causing an increased communication cost for the protocol. The network is flooded by the BS with a request message and the IDs of the nodes which are much affected. These nodes reply to the BS with a message including IDs, next hop ID and its cost. The sinkhole can be detected on the basis of that received information. Other protocols agree to detection methods for sinkhole attacks in sensor networks that are use routing protocols usually Ad Hoc Ondemand. Distance Vector Protocol (AODV) and the Dynamic Source Routing (DSR) Protocol [6]. As discussed above, this many-to-one message passing model is susceptible to sinkhole attacks. In sinkhole attack, an adversary usually gets the traffic of whole network by sending broadcast about its presence and pretends to a sink node for all nodes in the network or a node providing shortest path towards sink node. For example, a malicious node, with higher computational resources and communication power as compared to ordinary sensing node, and creates a better-quality single-hop link to nodes existing there. In the end, it broadcasts short routing messages regarding that high quality link, spoofing the neighboring nodes to create a sinkhole (SH). A sinkhole can also be created by using a wormhole, which creates a sinkhole with the attacker being the center; the intruder then forwards the messages toward the sink using a tunnel [4]. Most of the research has investigated and proposed mechanism for sinkhole attack in WSN; in contrast in this paper we investigate the sinkhole attack in BAN which utilizes the local information content from the data aggregation algorithm [7].

5 Detection of Sinkhole Attack

In this section, we propose our detection scheme for the sinkhole attack scenario illustrated in Section 3. We use the terminologies define in Table 3 to presents out idea.

5.1 Sinkhole Launching Strategy

From the attacker?s perspective the most important task to launch this attack in a single BAN scenario are as follows:

- Attacker SNK_Hole impersonates the original sink node *SNK*.

Table 3: Terminologies used by the algorithm

SN_i	Represents sensors nodes where i is its ID
SNK	Represents the original sink node
SNK_Hole	Represents the sink hole attacker
Req_Data	A packet sent from SNK to SNi to request data
TI	Time interval
n	Periods of data aggregation used for detection

- *SNK_Hole* sends a *Req_Data* packet to all SN_i.
- If impersonation successful then *SNK_Hole* will receive data from all nodes as a reply to *Req_Data* and will simply drop them to create the sink hole.
- Legitimate *Req_Data* received from *SNK* later will be processed then.

The data aggregation in BAN could be either

1) Periodic,
2) Event driven,
3) Combination of both periodic and event driven.

In periodic the *SNK* sends the *Req_Data* after a certain time period periodically for example in a general patient monitoring scenario where all body parameters needs to be monitor for maintaining patients history. On the other hand event driven data aggregation will trigger on the occurrence of certain event for example critical level of blood glucose is notice by the sensor. In this case the sensor node will transmit the data to *SNK*, from where it will be transmitted to doctors or to emergency service providers.

In both type of data aggregation schemes the above mention sinkhole launching strategy will work in the scenario illustrated in Section 3. Simply because if there is no means for the SN_i nodes to differentiate between authorize and un authorize sink then the *SNK_Hole* will receive all the data instead of *SNK*. Having a proper authentication procedure in place will certainly stop this type of attack. However, we learn from the literature that the cost of implementing such mechanism is generally are on the higher side for BAN application. Therefore, in this paper we assume there is no authentication service is in place and instead we propose to use the information from the data aggregation protocols to distinguish between and *SNK* and *SNK_Hole*.

5.2 Model Assumptions

We assume the sink hole attack scenario illustrated in Section 3. We assume energy efficient multi hop data aggregation technique such as DARE [17] in place. It uses the concept of relay nodes (a multihop scenario) to efficiently utilize the energy of the nodes in the network. It is a distance aware protocol means before the transmission of data it estimates the residual energy and distance between the sensors, relay and sink node. There are two possible placement of *SNK_Hole* attacker node:

1) On the body of the patient as illustrated in Figures 5 and 6;
2) Outside the body of the patient. We consider the later as in earlier case the patient will notice if extra sensors is attach to the body. We further assume the stationary sink node *i.e.* no mobility.

5.3 Core Functionality of Proposed Method

We now describe the core functionality of our detection mechanism. It mainly consists of two modules data aggregation and Sinkhole Detection.

5.3.1 Data Aggregation

The sink node sends a *Req_Data* to all the SN_i We employ energy efficient multi hop data aggregation technique in [15]. It estimates the transmission and reception energy using the basic radio model proposed in [5] are given below as Equations (1) and (2).

$$\begin{aligned} E_{TX}(k,d) &= E_{TX\,elec} \times k + E_{amp}(n) \times k \times d_n \quad (1)\\ E_{RX}(k) &= E_{RX\,elec} \times k. \quad (2) \end{aligned}$$

Here, E_{TX} in Equation (1) represents the transmission energy and Equation (2) calculates the receiving energy represented by E_{RX}. k represents the number of bits transmitted, d represents the distance. The radio energy dissipates by the transmitter and receiver is represented by $E_{TX\,elec}$ and $E_{RX\,elec}$. E_{amp} is the energy for the transmit amplifier and the d is the distance between sender and receiver.

We consider the scenario shown in Figure 3 and perform the data aggregation in the following steps:

- It first measure the distance between the SN_i and sink *SNK*.
- It then estimates the transmitted energy of sensor and received energy of relay node or sink.
- Based on the estimated energy and distance it selects the multihop path to aggregate data.
- This process continues until sense data from all the SN_i is received.
- It also maintains the residual energy of relay and *SNK* node.

5.3.2 Detection of Sinkhole

We consider the sinkhole launching strategy and data aggregation technique describe earlier. We propose to utilize the parameters related to energy and distance maintain during the data aggregation to identify the *SNK_Hole* attacker. We define the data aggregation is done periodically after each time interval *(TI)* for n periods. We use the concept of anomaly based detection, where we employ two mechanisms training and testing. In training we maintain the expected normal profile of the parameters from data aggregation in *EXPECTED* matrix. Testing process in invoked when training profile is build. In testing the algorithm maintain the current values of the parameters in *OBSERVED* matrix. During the testing *OBSERVED* matrix parameters are statistically compared with *EXPECTED* and in case of significant statistical deviation we declare the node as *SNK_Hole* attacker.

Algorithm 1 illustrate the propose sinkhole detection process in BAN. It requires the maintenance of two matrixes *OBSERVED* and *EXPECTED* with three parameters. Where the later represents the expected parameters values related to distance and energy of sink node and the earlier matrix represents the current information received from the node claiming to be sink. Since we consider the specific placement of sink node on the body, therefore technically these two matrixes should not be significantly different. To reduce the possibility of false detection we calculate the statistical deviation ($S.D$) based on observation from n periods. The algorithm is general and the detection parameters values such as number of parameters in two matrix?s, n and threshold could be modified to implement the algorithm in different scenarios.

5.3.3 Algorithm

Detection of sinkhole is done in the following steps:

- The detection module maintains the updated information regarding the relay and the *SNK* of data aggregation parameters.

- Repeat after each TI for n periods

  - Updated values of E_{TX}, E_{RX}, d, are kept in the textitSN_i as *EXPECTED* matrix.

    EXPECTED=$\{E_{TX}, E_{RX}, d\}$

  - When the SN_i receive the *Req_Data*, it will obtain the parameters from the data aggregation algorithm term as *OBSERVED* matrix. *OBSERVED*=$\{$O.E_{TX},O.E_{RX},O.d,$\}$ SN_i is received.

  - Compare the current values of distance and energy parameters from the algorithm regarding the sink node/ relay node with the previous information store in the table.

- End repeat

- Calculate statistical deviation SD using the Equation (3):

$$S.D = \frac{\sum_{i=1}^{n} OBSERVED_i - EXPECTED_i}{n}. \quad (3)$$

- If ($S.D >$ *threshold*) then

  we confirm the node as *SNK_HOLE*

  Else

  We conclude the node as genuine *SNK* Update *EXPECTED* matrix using Equation (4)

$$\forall_i(\overline{EXPECTED}^i_n) \quad (4)$$
$$= \alpha \times OBSERVED^i_n + (1-\alpha) \times \overline{EXPECTED}^i_n.$$

- End

We use exponentially weighted moving average to update matrices using Equation (4), where $\overline{EXPECTED}^i_n$ and $OBSERVED^i_n$ represents the expected and observed matrix with i parameters and n time interval. Here $\alpha = 2/(n-1)$ is the weighting factor.

5.4 Complexity Estimation of Proposed Method

Now we estimate the running time & complexity of proposed algorithms. We assume a single non-iterative task takes t seconds to complete. Total number of times the algorithm module runs is n *TIs*. Now we consider Algorithm 1 pseudo-code of sink hole detection phase, which can be split into three tasks for estimation of their time complexity.

1) Collecting and maintaining updated values of *EXPECTED* and *OBSERVED* matrices. Running time of this part can be estimated using further dividing into three tasks.

   a. Estimating and storing data for j parameters of *EXPECTED* matrix, so time complexity will be j * t.

   b. Obtaining and storing parameters from data aggregation algorithm for j parameters j*2*t.

   c. Comparing j parameters of matrices j*t.

   So the running time of task 1) is $= jt + j * 2t + jt = 4jt$ As this task repeats for n $TI = n * (4jt)$.

2) Calculation of statistical deviation of j parameters of two matrices.
   Running time of this part can be estimated using further dividing into two tasks.

   a. Calculating $S.D$ using equation in Algorithm 1 $j * n * t$.

   b. Comparison S.D computed and threshold values $j * t$.

So running time estimation for task 2) = $j(nt + t)$.

3) Update *EXPECTED* matrix.
Updating expected values $j * n * t$.
So running time estimation is $= j * n * t$.

Now combining task 1), 2) and 3).
Running Time (complexity) $= n(4jt) + j(nt + t) + jnt$.
Which can be simplified to Running Time (complexity) $= (6nj + j)t$.
If we remove constant then the expression in big-Oh notation will be $O(j(n+1))$. In general we can say that the running time complexity of the detection algorithm will depend on the j *(number of parameters in matrices)* and n *(the number of data aggregation periods)*. This could also give us the estimate of cost of the detection algorithm in the scenario it is implemented.

6 Performance Evaluation

We now present the performance analysis of BAN under sink hole attack and the result of our detection algorithm. We have used Castalia which is based on OMNET ++ platform to simulate the BAN scenario. We consider the BAN in Figure 2 and create a simulation scenario using the simulation parameter in Table 4. Each node in our scenario sends certain number of packets per seconds for the simulation time. We run our scenarios first with no sink hole attack then intentionally created a sinkhole attack to analyze its effect on network performance using packet received, latency and packet breakdown (errors) as basic parameters. We run these scenario with GTS is turn on or off along with either temporal channel (*i.e.* path loss exists) and no temporal channel (*i.e.* no path loss exists).

Table 4: Simulation parameters

Parameter	Value
No of nodes	6 nodes, node 0 is sink
Transmit Power	-15dB
Simulation Time limit	600 sec
Start up delay	1 sec
Packet rate	30 pkt/sec

All our simulation is performed using the body area network scenarios shown in Figure 2 with six sensors are placed at different parts of the body. We use the simulation parameter in Table 4. The graph in Figure 7 shows the results of the normal scenario (no attack) with packet received per node (all nodes send their data to node zero so the term per node is used). The graph shows variations in the number of packets received by six nodes in the network with respect to the various GTS options. The graphs show GTS on with no temporal has slightly better performance as compare to other GTS options. In this scenario we assume there is no attack in the network, therefore, the graph reflects the normal behavior of nodes in the network. Figure 8 demonstrates the second case in which we have introduced sinkhole attack. In this case where an attacker node acts as a sink node; as a result the GTSon General and GTSoff General curves have fallen drastically because the node 6 is dropping all the packets which it receives from the neighboring nodes. This shows the significant degradation in the network performance. In this scenario we introduce sink hole attack and the drastic change of performance in terms of received packets per node is evident. We have also observe the latency in both scenarios (*i.e.* with and without sink hole attack), Figure 9 and 10 shows the effects of sinkhole attack on latency. We can see the graph in Figure 9 the latency of majority of the packets is less than 100ms, it shows those packets transmitted in the first MAC frame. In this case no temporal performs better but there is some saturation in temporal case. However, the graph in Figure 10 shows the packets received within the first attempt are quite good in number but later on there are large number of packets with large delay. There is a huge latency shown in general case but a considerable increase is shown in

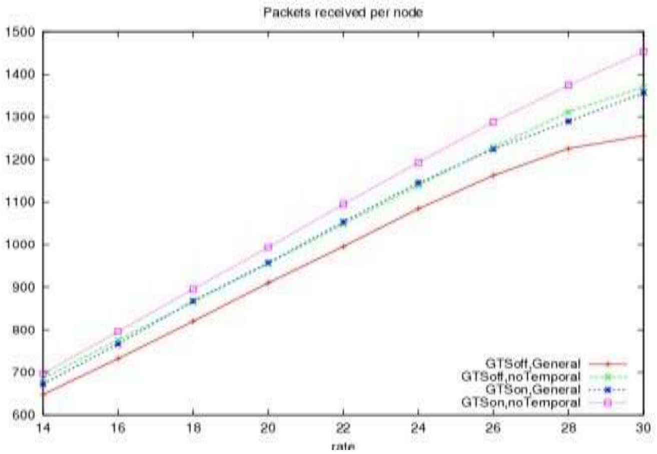

Figure 7: Packets received per node with no sinkhole

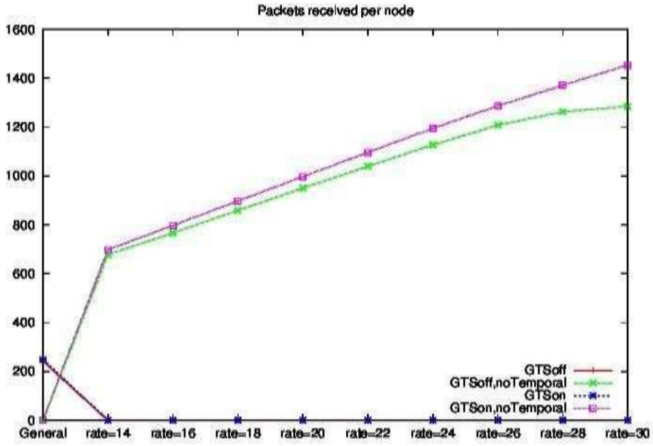

Figure 8: Packets received per node with sinkhole

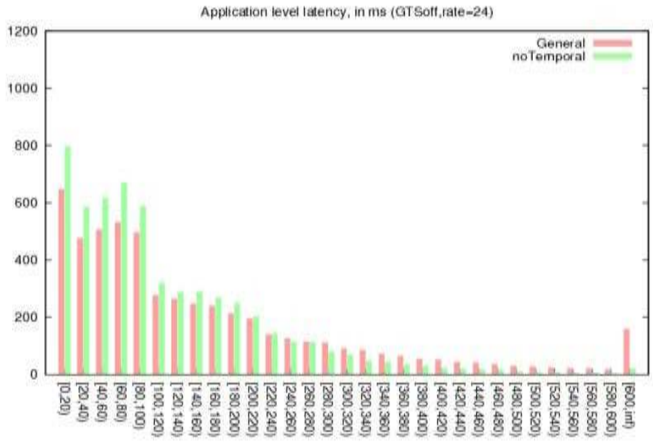

Figure 9: Latency in general and no temporal (GTSoff) with no sinkhole

noTemporal case. Analyzing the effect of the presence of

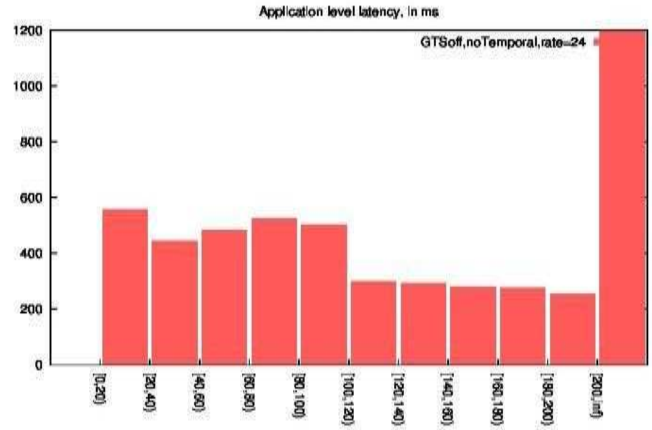

Figure 10: Latency in General and noTemporal (GTSoff) with no sinkhole

sinkhole attack on packet latency from graphs in Figures 9 and 10 clearly shows the degradation of performance with sink hole attack in the network.

We have also analyzed the Packet breakdown with both scenarios (with and without attack). The graphs in Figure 11 show that the most of the packets failed because of noAck (a direct result of the deep fades in the channel and loss of connectivity) and overflow in the case of high rates. The packet drop rate of busy channel and buffer overflow is negligible, but 90% of the packets are received in successfully. There are almost 80% of total packets received properly in first try because there is no attacker in this case. The graphs in Figure 12 show that the most of the packets failed because of buffer overflow because the attacker is creating such a condition and going to drop the packets and this overflow occurs due to high rates. The packet drop rate of busy channel and buffer overflow is almost 50%. There is 40% more packet loss in the first try because of sinkhole attack and this clearly indicates the degradation of performance in the network.

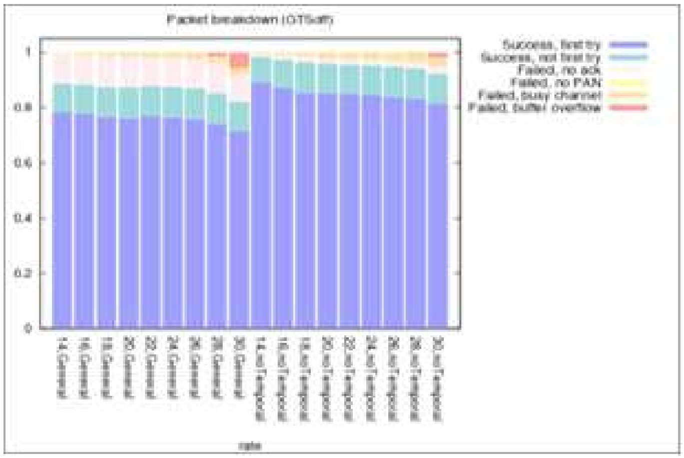

Figure 11: Packet breakdown in noTemporal (GTSoff) without sinkhole

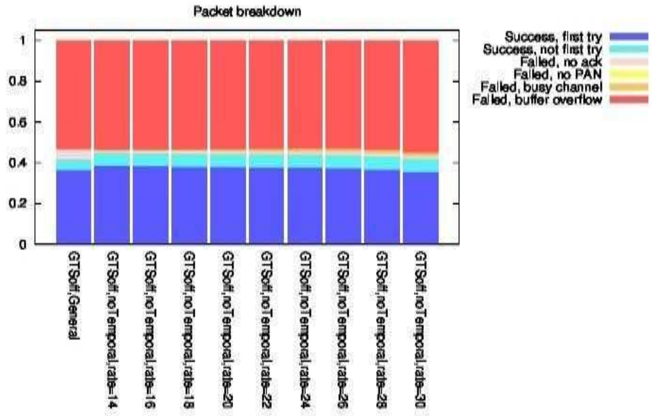

Figure 12: Packet breakdown in noTemporal (GTSoff) with sinkhole

To sum up this simulation performance evaluation indicates that the sinkhole attack could severely degrade the performance of the network.

In the final set of experiments we implemented our propose sink hole detection algorithm using the same simulation parameters in Table 4. We simulated the scenario with data aggregation technique of [7] and radio model of [5] and introduce the *SNK_HOLE* during the simulation in the network. We perform 10 runs each set of experiments with sink hole attack introduce in the network and observe the detection rates of success and false alarm. The graph in Figure 13 shows success and false alarm rate in the five set of experiments. Success rate here means that the *SNK_HOLE* attacker was detected successfully during the experiments. False alarm rate means the number of time the normal node or genuine sink node is detected by the algorithm as attacker. The graph in general shows the high success and low false alarm rate of our proposed algorithm. The major issue with anomaly based detection scheme is high false alarm rates; therefore we have declared detection based on the outcome of n periods instead of a single run.

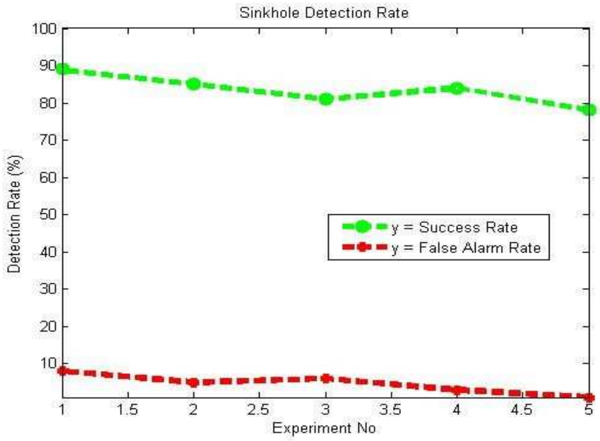

Figure 13: Detection rates of proposed sink hole detection algorithm

7 Conclusion & Future Work

Wireless body area sensor network is emerging technology that has applications in major walks of life especially in healthcare. However, BAN operations are vulnerable to security attacks. Considering the security requirement of healthcare application of BAN, in this paper we have analyze the performance of the BAN under sinkhole attack scenario. We propose the sink hole attack detection algorithm that utilize the distance and energy related information from the data aggregation technique to detect the sink hole attack in BAN. The simulation base study shows that this attack could severely degrade the performance of the network in terms of low throughput, higher delay and packet breakdown. Simulation results show good performance of our detection algorithm in terms of high detection and low false alarm rates.

In future our focus is on investigating security and privacy issues in multi BAN scenario applied to hospital ward. That is to use the multi BAN to remotely monitor all the patients in a ward using the wearable shimmer sensors. Then study, identify and propose solution for the privacy and security issues in this scenario.

Acknowledgments

We acknowledge the efforts of MS student Mr Ghullam Abbas in terms of simulation scenarios of performance analysis.

References

[1] F. Agrafioti, F. M. Bui, and D. Hatzinakos, "On supporting anonymity in a ban biometric framework," in *16th International Conference on Digital Signal Processing*, pp. 1–6, 2009.

[2] M. A. Ameen, J. Liu, and K. Kwak, "Security and privacy issues in wireless sensor networks for healthcare applications," *Journal of Medical Systems*, vol. 36, no. 1, pp. 93–101, 2012.

[3] S. Bouchkaren and S. Lazaar, "Caes cryptosystem: Advanced security tests and results," *International Journal of Network Security*, vol. 20, no. 1, pp. 177–183, 2018.

[4] Boulis, A. Castalia, *A Simulator for Wireless Sensor Networks and Body Area Networks*, ver. 2.2. User's Manual, NICTA: Canberra, Australia, 2009.

[5] B. Braem, B. Latre, I. Moerman, C. Blondia, E. Reusens, W. Joseph, L. Martens, and P. Demeester, "The need for cooperation and relaying in short-range high path loss sensor networks," in *International Conference on Sensor Technologies and Applications*, pp. 566–571, 2007.

[6] M. Deylami and E. Jovanov, "Performance analysis of coexisting ieee 802.15. 4-based health monitoring wbans," in *Annual International Conference of the IEEE Engineering in Medicine and Biology Society*, pp. 2464–2467, 2012.

[7] N. Javaid, Z. Abbas, M. S. Fareed, Z. A. Khan, and N. Alrajeh, "M-attempt: A new energy-efficient routing protocol for wireless body area sensor networks," *Procedia Computer Science*, vol. 19, pp. 224–231, 2013.

[8] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: Attacks and countermeasures," *Ad Hoc Networks*, vol. 1, no. 2-3, pp. 293–315, 2003.

[9] O. U. O. Khan, A. Nadeem, K. Ahsan, and N. Mehmood, "Rprp: Reliable proactive routing protocol for wireless body area sensor network," *Journal of Basic and Applied Scientific Research (JBASR'14)*, vol. 4, pp. 17–25, 2014.

[10] M. Li, W. Lou, and K. Ren, "Data security and privacy in wireless body area networks," *IEEE Wireless Communications*, vol. 17, no. 1, pp. 51–58, 2010.

[11] A. Nadeem and M. P. Howarth, "A survey of manet intrusion detection & prevention approaches for network layer attacks," *IEEE communications Surveys & Tutorials*, vol. 15, no. 4, pp. 2027–2045, 2013.

[12] J. Qi, T. Hong, K. Xiaohui, and L. Qiang, "Detection and defence of sinkhole attack in wireless sensor network," in *IEEE 14th International Conference on Communication Technology (ICCT'12)*, pp. 809–813, 2012.

[13] A. Salam, A. Nadeem, K. Ahsan, M. Sarim, and K. Rizwan, "A novel QoS algorithm for health care applications of body area sensor networks," *Textroad Journal of Basic and Applied Scientific Research*, vol. 4, no. 1, pp. 169–178, 2014.

[14] S. A. Salehi, M. A. Razzaque, P. Naraei, and A. Farrokhtala, "Detection of sinkhole attack in wireless sensor networks," in *IEEE International Conference on Space Science and Communication (IconSpace'13)*, pp. 361–365, 2013.

[15] R. Singh and M. S. Manu, "An energy efficient grid based static node deployment strategy for wireless sensor networks," *International Journal of Electronics and Information Engineering*, vol. 7, no. 1, pp. 32–40, 2017.

[16] M. Styugin, "Establishing systems secure from research with implementation in encryption algorithms," *International Journal of Network Security*, vol. 20, no. 1, pp. 35–40, 2018.

[17] A. Tauqir, N. Javaid, S. Akram, A. Rao, and S. N. Mohammad, "Distance aware relaying energy-efficient: Dare to monitor patients in multi-hop body area sensor networks," in *Eighth International Conference on Broadband and Wireless Computing, Communication and Applications (BWCCA'13)*, pp. 206–213, 2013.

[18] Y. Tian, Y. Peng, G. Gao, X. Peng, "Role-based access control for body area networks using attribute-based encryption in cloud storage," *International Journal of Network Security*, vol. 19, no. 5, pp. 720–726, 2017.

[19] C. Tumrongwittayapak and R. Varakulsiripunth, "Detecting sinkhole attacks in wireless sensor networks," in *ICCAS-SICE*, pp. 1966–1971, 2009.

[20] I. C. Weng and T. H. Chen, "A novel weighted visual cryptography scheme with high visual quality.," *Internationl Journal Network Security*, vol. 19, no. 6, pp. 922–928, 2017.

Biography

Dr. Adnan Nadeem is currently working as an Associate Professor in the Faculty of Computer Science and Information System, Islamic University in Madinah, KSA since 2016. He is also associated with Federal Urdu University of Arts Science & Technology, Pakistan since March 2011. During this period, he earned several research grants. He was awarded 5th HEC Outstanding Research Award 2013/14 for his paper published in IEEE Journal of Communication Survey and Tutorials (Impact Factor=17.18). During his pedagogical journey he has won several awards and achievements including the Foreign PhD scholarship, Associate Fellowship of Higher Education Academy (AFHEA), UK in 2009 and best paper & best paper of the track award in the ICICTT 2013 and ICEET 2016 conferences, respectively. He was awarded "Nishan-e-Imtiaz" for his outstanding research by Federal Urdu University Pakistan on August 2016. He received his PhD degree from Centre for Communications Systems Research, (CCSR) University of Surrey, UK in 2011. He has published more than 40 papers in international conference and journals. His research interests include WBAN applications in healthcare, agriculture and disability assistance. He also worked in security, routing and QoS in MANET and WSN.

Turki Alghamdi is currently working as an Assistant Professor, the Dean, and the Founder of the Faculty of Computer and Information Systems at Islamic University in Madinah, KSA. He received a BSc in Computer Science from Taif University, KSA in 2005, and MSc in Software Engineering from University of Bradford, UK in 2008 . He received a PhD in Software Engineering from De Montfort University, UK in 2012.