Journal of Computer Science 6 (11): 1355-1361, 2010
ISSN 1549-3636

A Novel Intrusion Detection System for Wireless Body Area Network in Health Care Monitoring

T.V.P. Sundararajan and A. Shanmugam
Department of Electronics and Communication Engineering,
Bannari Amman Institute of Technology, Sathyamangalam, 638402, India

Abstract: Problem statement: Health monitoring, telemedicine, military, interactive entertainment and portable audio/video systems were most promising applications where WBANs can be used. However, designers of such systems face a number of challenging tasks, as they need to address often quite conflicting requirements for size, operating time, precision and reliability. Network security is very important in Wireless Body Area Network (WBAN) since the vital human life might be jeopardized, unless managed properly. **Approach:** This article presented security architecture of a wireless body area network for ambulatory health status monitoring. A novel Intrusion Detection System (IDS) inspired by the biological immune system that use Negative Selection Algorithm (NSA) was proposed to enhance the performance of Wireless Body Area Networks (WBAN) to operate despite the presence of compromised (misbehaving) nodes. **Results:** The proposed IDS scheme had been implemented using network simulator Qualnet v5.2. The performances of IDS scheme had been analyzed using AODV, DSR and DSDV routing protocols for parameters such as average detection rate and false alarm rate. These negative selection detectors are capable of distinguishing well behaving nodes from compromised nodes with good degree of accuracy. The high false positives rate is also minimized. **Conclusion/Recommendations:** Wireless Body Area Networks are an enabling technology for mobile health care. The IDS can be implemented on today's devices as it only requires minimal and low-cost hardware changes. The authors strongly believe that adding sufficient security mechanisms to WBAN will study as a trigger in the acceptance of this technology for health care purposes. Simulation results indicate the non-degradability of network performance when these IDS is incorporated in the routing algorithm for security enhancements.

Key words: Wireless body area network, intrusion detection, health care, DSR, AODV and DSDV

INTRODUCTION

Wireless Body Area Networks (WBANs) allow the integration of low-power, miniaturized, invasive/noninvasive wireless sensor nodes in/around a human body to monitor patient's vital signs for real-time diagnosis and prescription. Each intelligent sensor node or BAN Node (BN) forwards data to a central coordinator also called BAN Network Controller (BNC). The BNC processes the data and forwards it to a medical server/physician for relevant recommendations. The deployment of WBANs for medical and non-medical applications should satisfy the stringent security and privacy requirements (Morchon and Baldus, 2008). Since the WBAN is used for monitoring and transmitting vital sign, measuring and increasing the security of WBAN is very important research issue. Malicious users may try to modify the patient information such as vital sign and patient ID, using security attacks such as denial of service compromised attack, wormholes and spoofing (Rahman *et al*., 2005). Failures may be caused by power exhaustion as well as these malicious security attacks. Since medical BAN applications have substantial financial, privacy and human safety implications, WBAN nodes should be protected from aforementioned failures and malicious attacks (Halperin *et al*., 2008).

Related study: In the context of security mechanisms in WBANs, such as intrusion detection and fault tolerant system, few of them are proposed to detect compromised sensors. Security management in WBAN consists of the intrusion prevention and intrusion detection. The intrusion prevention is the first line of defense, such as encryption and authentication mechanisms and so on. The mechanisms provide the

Corresponding Author: T.V.P. Sundararajan, Department of Electronics and Communication Engineering,
Bannari Amman Institute of Technology, Sathyamangalam, 638402, India

function of authentication and encryption by using the key of a time interval (Liu and Ning, 2003). They depend on less storage capacity and they are very efficient to defend many attacks in the WSNs. The intrusion detection is the second line of defense, such as DoS detection and so forth. Many investigations on detecting DoS attacks are proposed, defining compromised node and designing an effective detection model. Intrusion detection mechanisms can be used to identify the intruded sensor nodes. Onat and Miri (2005) proposed an IDS system, where sensor nodes in the network are responsible for monitoring their neighbors and looking for intruders. Bhuse and Gupta (2006) proposed some straightforward and efficient detection at all protocol layers. Da Silva *et al*. (2005) proposed a decentralized IDS that is based on the inference of the network behavior obtained from the analysis of events detected by a monitor node, i.e., the node that implements the IDS system. Due to the characteristics of low power, low computation ability, low storage space, simplicity and high-efficiency is our design goal. Only when compromised sensors can be detected, the WBANs could be safer in practice. This research propose a anomaly detection model, making use of a negative selection detection mechanism (Khor *et al*., 2009) and the information of each layer in the communication protocol to detect which sensors are already compromised.

MATERIALS AND METHODS

WBAN security threats: Denial of Service (DoS) attacks affect the capacity and the performance of a WBAN. One of the security threat is the modification of data. This occurs when an unauthorized entity inserts, changes, or deletes information transmitted between nodes in WBAN. This is an attack on integrity and can result in a DoS attack or man-in-the-middle attack (Karlof and Wagner, 2003; Perrig *et al*., 2002). For example if health information of a patient is modified, he can get a wrong disease or be unaware about a disease due to false information. This results a great disaster. In this research study, two familiar Denial of Service (DoS) attacks were implemented in simulation: (1) Denial of service attack from an attacker machine outside the WBAN and (2) Denial of service attack from a compromised machine inside the WBAN.

WBAN system model: The architecture of WBAN is divided into three Levels as shown in Fig. 1 the first level is consists a set of intelligent sensors or BAN Nodes (BN) which are the reduced function devise. In the non-medical field, wearable devices such as a headset, mp3 player, a game controller can be included in this level. Level 1 BNs can have local storage temporarily. The second level is the BAN Network Controller (BNC) mobile personal server that has full function devices like Internet enabled PDA, a cell-phone. It communicates with the external network and temporarily stores the collected data from the lowest level devices. Additionally, it can display the analyzed information on a screen with an option. Level 2 BNCs have enough storage to save measured data and the ability to upload and download these data from external server. The third level includes Home Server (HS) and external network of remote servers which provides various application services. For example, the medical server keeps electronic medical records of registered users and provides various services to the users, medical personnel and informal caregivers. Since BNC study as a part of a firewall, a personal storage of vital information and point of intersection of network protocols, this research study focus to implement IDS of each BNC and Home server.

If the BNC's cryptographic key is compromised, an attacker may monitor and control it unscrupulously. It is very dangerous in that situation. So we need some model to guard against such situation. The compromised BNCs we observed almost issue some abnormal messages and attack other normal sensors actively. In this study, we proposed the IDS model for WBAN. Figure 2 shows the environment and detection mechanism. The white, black and server represents normal BNC and compromised BNC and Home Server (HS) respectively.

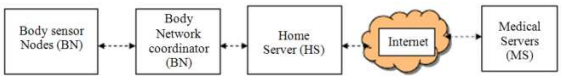

Fig. 1: Architecture of WBAN

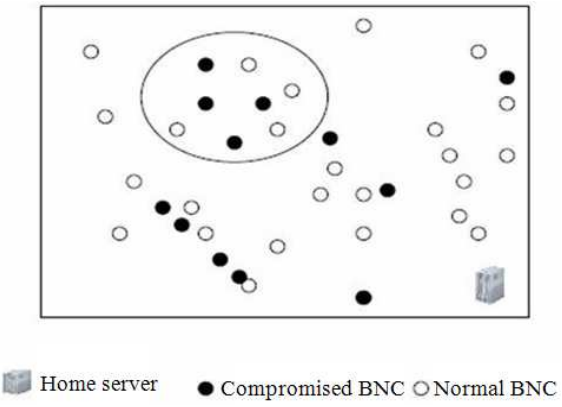

Fig. 2: System model

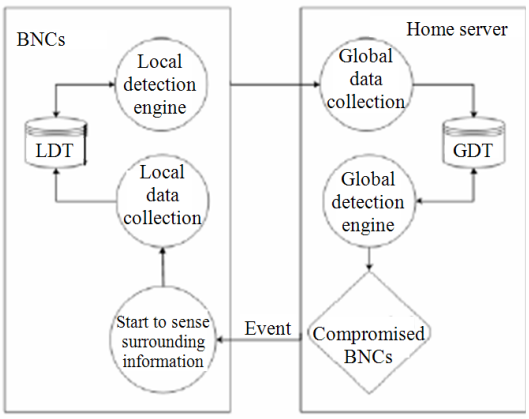

Fig. 3: System architecture

The big cycle represents the event region. When sensors belong to each BNC begin to sense surrounding information, they will execute anomaly detection mechanisms at BNC level and then send messages to the HS. When the HS receives a message from a BNC, it will execute anomaly detection mechanisms to decide if the BNC is compromised or not. Finally, the compromised nodes are detected at the HS.

The proposed system architecture is shown in Fig. 3. Two tables are defined to store communication information among sensors and base station: Local Detection Table (LDT) and Global Detection Table (GDT). The LDT which is built for preparing the information for individual detection mechanisms at each individual BNC. In addition, the GDT which is built for storing all BNC's information and the result of the detection model is stored in the HS. This mechanism is triggered by events. Finally, the HS detects the compromised BNCs.

Detection mechanism: The basic premise for anomaly detection is that there is intrinsic and observable characteristic of normal behavior that is distinct from that of abnormal behavior. Negative Selection Algorithm (NSA) is used as detection algorithms to build anomaly detection models. Using this Architecture, the following procedure for anomaly detection is employed: (a) select audit data (b) perform appropriate data transformation according to the entropy measures (c) compute detector using training data; (d) apply the detector to test data and (e) post-process alarms to produce intrusion reports.

Negative Selection Algorithm (NSA): The Negative Selection Algorithm (NSA) is based on the principles of self/non-self discrimination in the immune system (Khor *et al*., 2009). It can be summarized as follows:

- Define self as a collection S of elements in a feature space X, a collection that needs to be monitored. For instance, if X corresponds to the space of states of a system represented by a list of features, S can represent the subset of states that are considered as normal for the system
- Generate a set F of detectors, each of which fails to match any string in S
- Monitor S for changes by continually matching the detectors in F against S. If any detector ever matches, then a change is known to have occurred, as the detectors are designed not to match any representative samples of S

Anomaly detection: The anomaly detection process aims at distinguishing a new pattern as either part of self or non- self, given a model of the self (normal data) set. The problem space, denoted by X in an n-dimensional space; the self set is denoted as S and let N be the complementary space of S It is assumed that each attribute is normalized to [0, 1]:

Then:

$$S \subseteq [0,1]^n \; S \cup N = X, \; S \cap N = L$$

Given the normal behavior of a system S the characteristic function of S defined as:

$$N_S(p) = \begin{cases} 1, \; p \in S \\ 0, \; p \in N \text{ is used to distinguish} \\ \text{between self and non-self} \end{cases}$$

Denial of Service (DoS) attack models: WBAN suffers from some inherent flaws and are therefore prone to more attacks than IEEE 802.15 WPAN networks because of some inherent security vulnerabilities and the stringent resource constraints in BANs. The negative detectors can be used to detect following Denial of Service (DoS) attacks: (1) Denial of service attack from an attacker machine outside the WBAN and (2) Denial of service attack from a compromised machine inside the WBAN. These two attacks were implemented using network simulator tool called Qualnet v 5.2. (Ahmed *et al*., 2007) as shown in Fig. 4.

Figure 5 shows a scenario with 10 nodes and the traffic flow among them. This scenario comprises of an WBAN with six wireless nodes communicating with each other as shown in Fig. 4 and established normal traffic flow. An attacker machine launches a PING flood attack to a wireless node. The Internet Control Message Protocol (ICMP) packet sequence numbers are collected at the Ad-hoc node different from the victim machine, which keeps pinging, on the victim machine throughout the experiments. The time taken for each packet to reach the destination node is noted when each ping (ICMP)

packet is sent. It is observed that during the occurrence of an attack, there are some drops in the ICMP packets. In addition, the time taken to reach the destination host increased when the attack was launched.

These nodes are labeled, ranging from Node 0 to Node 9. Constant Bit Rate (CBR) traffic is defined between Node 0 and Node 2 Node 3 to Node 4, Node 4 to Node6, Node 5 to Node 3 Node 6 to Node 7, Node 1 to Node 8, Node 9 to Node 2, Node 8 to Node 7 and File Transfer Protocol (FTP) traffic flows between Node 1 and Node2. The start times for all these traffics are preset. The attack is launched from Node 0 to Node 2. The attack is simulated as DoS with heavy traffic flow in a short time interval. During these periods when the attack was launched, the number of legitimate packets received by the victim node (Node 2) was reduced. The sequence numbers resulting from the connection between different nodes and Node 2 were collected.

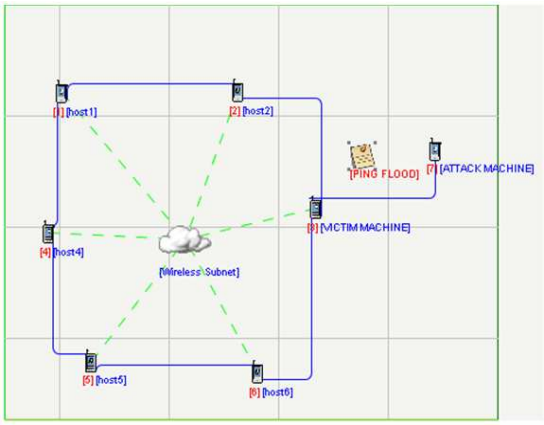

Fig. 4: DoS attack from external compromised BNC

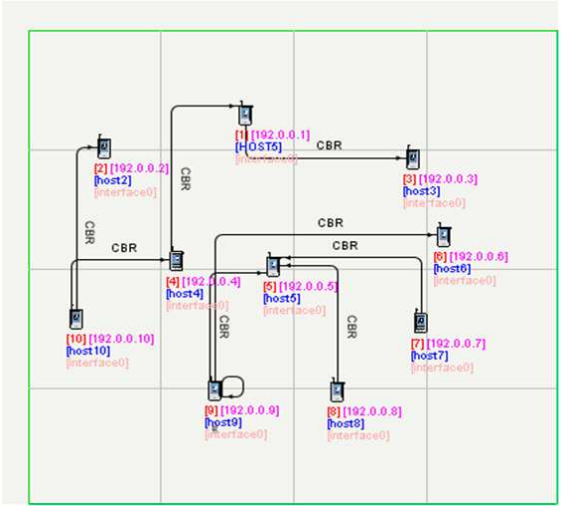

Fig. 5: DoS attack by an internal compromised BNC

Learning and detecting process: During the learning phase, all the nodes (BNCs) were made to behave well so that a generated profile for the entire network traffic could be built and negative detectors could be generated and trained. The simulation time was set for a long duration, so as to capture a considerably large and proper profile of the system as also to collect sufficient good behavior, which is an important concern for anomaly detection problems. During the detection phase, certain numbers of nodes (BNCs) were made to misbehave. The trained detectors were tested against this behavior towards the end of the simulation for the rate of detection and false positives in misdetection of the well behaved BNCs. Different set of parameters as shown in Table 2 were used for the detection phase in deciding detection rate and the false positive classification rates. A critical parameter called the learning data threshold was used for the purpose to keep a balance between high detection rate and low false alarm rate. This parameter is applied to each data point (a data point is a vector of 4 dimension data) so as to generalize the overall profile.

RESULTS

Qualnet v 5.2 network simulator (Ahmed *et al*., 2007) has been used to analyze the reactive routing protocols DSR, AODV and DSDV. The under lying MAC protocol defined by IEEE 802.11 was used Traffic sources of both Continuous Bit Rate (CBR) based on TCP for 10 sources were generated. The CBR and TCP mobility scenario of 20 nodes with a maximum speed of 20 sec and for a simulation area of 500×500 with 4.0 kbps was generated. Each model had five scenario files generated with different pause times of 0, 10, 30, 40 and 50 sec.

Experimental details: The incorporation of misbehavior into the network is explained as follows: The nodes can be set to misbehave as a Boolean parameter. It can be set or reset. Using this implementation capability each scenario could have different numbers of misbehavior nodes set up (in this experiments, 5, 10 and 20 were involved). The misbehavior are implemented in two ways (1) Nodes neither forward route requests nor answer the route replies from their route cache. (2) The nodes do not forward data packets. The misbehavior probability is a control parameter such that the misbehaving nodes behave badly only during certain times in the simulation run. The same or different probabilities could be utilized in either case. To study the feasibility of proposed negative selection algorithm based

anomaly intrusion detection system, series of experiments were conducted to evaluate its effectiveness. The anomaly detection methods can be applied to the DSR, AODV and DSDV routing protocols (Sharieh *et al*., 2008) and demonstrate the effectiveness of proposed model on different scenarios. For data set collection, detection and analysis, crucial simulation and detection parameters, as defined in Table 1 and 2 were used.

Performance analysis metrics: The experimental simulation aims at finding and reporting the detection behavior of the generated nodes in correctly identifying the misbehaving nodes as well as how well it could identify such deviations in behavior. The experimental results are based on the following metrics:

- Average detection rates for the misbehaving nodes is defined as:

  Detection Rate (DR) = (true positives)/(true positives + false negatives)

- Average False Alarm rates for misclassifying the well behaving nodes is defined as False Alarm Rate (FAR) = (false positives) / (false positives + true negatives)

Table 1: Simulation system parameters

Parameter	Default values
Routing protocol	DSR, AODV and DSDV
Simulation time	60 min
Simulation area in meters	800×1000 m
Number of nodes	60
Radio range	380 m
Propagation Path loss model	Two-ray
Mobility model	Random
Mobility speed (no pauses)	1 m sec^{-1}
Misbehaving nodes	10, 20, 30, 40
Traffic type	TELNET, CBR
Payload size	512 bytes
Frequency/rate	0.2-1 sec
Radio-Bandwidth/link speed	2 Mbps

Table 2: Detection system parameters

Parameter	Default value (s)
Upper limit for events sequence sets of a monitored node for learning	500
Number of subsequence in a sequence set	4
Upper limit for the number of events in a sequence set	40
Upper limit for a sequence set collection	10 sec
Misbehavior probability	0.8
Two-ray Learning data threshold	0.001-0.1
Threshold for detection (% of detection rate)	0.25
Mutation probability	0.05-0.1
Crossover probability	0.6
Normalized space range	[0.0, 1.0]
Number of dimensions	4

Where, true positives refer to the number of abnormal cases identified as abnormal in the given data set of vector points. False positives refers to the number of normal cases mistakenly identified as abnormal; true negatives refer to the number of normal event sequences (normal cases) in the entire sequence correctly identified as normal while false negatives are the count of the number of those abnormal sequences that the detector set classified as normal. Whenever and wherever we refer to positive detection and misclassifications, we refer to these metrics respectively.

DISCUSSION

Based on the Performance metrics, the following results are presented here for clarity. It is interesting to observe that DSR with its results outperforms AODV, DSDV protocols a lot, while the DSDV is the worst. The simulation scenario as shown in Fig. 4 and 5 demonstrate that a behavior based anomaly detection approach can study well on different WBANs. That is, the normal behavior of a routing protocol can be established and used to detect compromised nodes.

Having done the simulations on three ad-hoc routing protocols, effort is now made to answer this question- which type of protocol is “better” for protocol in which a degree of redundancy exists within its infrastructure. DSR embeds a whole source route in each packet dispatched, hence making it harder to hide the intrusion by faking a few routing information. This route update depends on traffic demand, which makes it misbehavior detection. The obtained solution tends to prefer DSR and AODV, even in the first look its route update is not as “regular” as DSDV. After detail analysis of these protocols, it is believed that misbehavior detection works better on a routing is due to path redundancy. Further, the DSR and AODV possible to establish relationships between routing activities and traffic pattern. This is called as pattern redundancy. DSDV, in contrast, has a very weak correlation between control traffic and data traffic, even when the traffic feature is preserved. Note that DSR and AODV are both on demand protocols. Therefore it is believed that those types of redundancy have helped on-demand protocols to have a better performance.

Detection capabilities: In all these experiments, average detection rates as shown in Fig. 5. 12 were substantially higher than the detection threshold. This demonstrates that all misbehaving nodes were detected and classified as misbehaving while the well-behaving nodes were classified as normal. Depending on the detector sets the average rates of detection and average false alarm rates (misclassifications) as in Fig. 6 and 7 were close to the median of the best and worst cases.

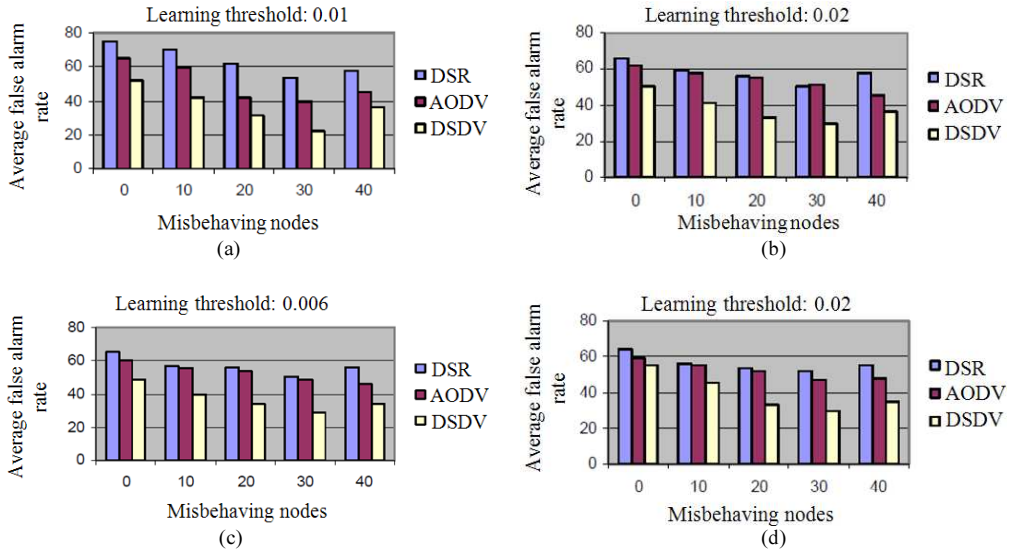

Fig. 6: Detection performance of DSR, AODV and DSDV

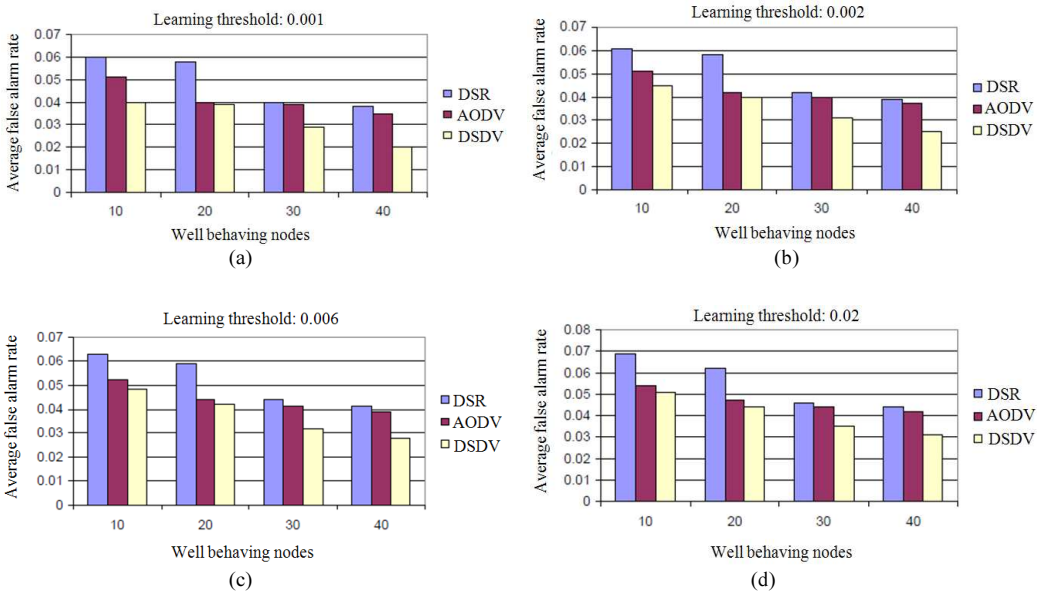

Fig. 7: False alarm rates of DSR, AODV and DSDV

It is showed that average false alarm rate as a function of number of misbehaving nodes. It can be observed that the average false alarm rate reduces as number of well behaving nodes increases for DSR, AODV and DSDV protocols. However, a false alarm rate of DSR is greater than AODV, DSDV for various threshold values. This is due to the fact that routes are broken frequently when the network is under the influence of Denial of Service attacks.

Impact of the learning threshold parameter: It is clearly observed from the experimental results that most of the misbehaviors are subtle and hence difficult to distinguish from the benevolent behaviors. This results in high false negatives thus lowering the detection rates. Thus a lower threshold value (0.001) has a higher detection rate compared to the higher ones. For a given learning threshold value, the number of misbehaving nodes also play a distinguished role. As

the number of misbehaving nodes increases, the detection rates decrease slightly.

CONCLUSION

WBAN reduce the enormous costs associated to patients in hospitals as monitoring can take place in real-time even at home and over a longer period. A critical factor in the acceptance of WBANs is the provision of appropriate security and privacy protection of the wireless communication medium. The data traveling between the sensors should be kept confidential and integrity protected. In this study we have presented novel IDS for Wireless Body Area Networks. It combines intrusion detection and secure routing techniques. It is believed to be the first attempt to model IDS for compromised BNCs in WBAN which is very efficient and secure for WBAN. It is found that the average detection rate for DSR is better rather than AODV and DSDV because behavior of DSR reflects the correlation between traffic pattern and routing message flows. However performance of the DSR is very sensitive to some detection parameters that require careful tuning. For average false alarm rate, DSDV perform better than DSR and AODV as the well behaving nodes increases. This is due to periodic update of traffic messages. Further research study work may include performing correlation studies between real test-bed measurements and simulation results.

REFERENCES

Ahmed, S., M. Bhilal, U. Farooq and Fazl-e-Hadi, 2007. Performance analysis of various routing strategies in mobile ad hoc network using QualNet simulator. Proceeding of the IEEE International Conference on Emerging Technologies, Nov. 12-13, IEEE Xplore Press, Islamabad, pp: 62-67. DOI: 10.1109/ICET.2007.4516317

Bhuse, V. and A. Gupta, 2006. Anomaly intrusion detection in wireless sensor networks. J. High Speed Networks, 15: 33-51. http://portal.acm.org/citation.cfm?id=1140567

Da Silva, A.P.R., M.T.H. Martins, B.P.S. Rocha, A.A.F. Loureiro and L.B. Ruiz *et al*., 2005. Decentralized intrusion detection in wireless sensor networks. Proceeding of the 1st ACM International Workshop on Quality of Service and Security in Wireless and Mobile Networks, Oct. 13-13, ACM Press, Montreal, Quebec, Canada, pp: 16-23. DOI: 10.1145/1089761.1089765

Halperin. D., T. Kohno, T.S. Heydt-Benjamin, K. Fu and W.H. Maisel, 2008. Security and privacy for implantable medical devices. IEEE J. Perv. Comput., 7: 30-39. DOI: 10.1109/MPRV.2008.16

Karlof, C. and D. Wagner, 2003. Secure routing in wireless sensor networks: Attacks and countermeasures. Ad Hoc Networks, 1: 293-315. DOI: 10.1016/S1570-8705(03)00008-8

Khor, K.C., C.Y. Ting and S.P. Amnuaisuk, 2009. From feature selection to building of Bayesian classifiers: A network intrusion detection perspective. Am. J. Applied Sci., 6: 1948-1959. DOI: 10.3844/.2009.1948.1959

Liu, D. and P. Ning, 2003. Efficient distribution of key chain commitments for broadcast authentication in distributed sensor networks. U.S. Army Research Office. http://www.isoc.org/isoc/conferences/ndss/03/proceedings/papers/17.pdf

Morchon, O.G. and H. Baldus, 2008. Efficient distributed security for wireless medical sensor networks. Proceeding of the International Conference on Intelligent Sensors, Sensor Networks and Information Processing, Dec. 15-18, IEEE Xplore Press, Sydney, NSW, pp: 249-254. DOI: 10.1109/ISSNIP.2008.4761995

Onat, I. and A. Miri, 2005. An intrusion detection system for wireless sensor networks. Proceeding of the IEEE International Conference on Wireless and Mobile Computing, Networking and Communications, Aug. 22-24, IEEE Xplore Press, USA., pp: 253-259. DOI: 10.1109/WIMOB.2005.1512911

Perrig, A., R. Szewczyk, J.D. Tygar, V. Wen and D.E. Culler, 2002. SPINS: Security protocols for sensor networks. Wireless Networks, 8: 521-534. DOI: 10.1023/A:1016598314198

Rahman, M.A., M.U. Mahfuz, K.M. Ahmed and R.M.A.P. Rajatheva, 2005. ICT based Sustainable rural business opportunities in developing countries: A wireless-networked RCP-RAP approach. Am. J. Applied Sci., 2: 1256-1260. DOI: 10.3844/.2005.1256.1260

Sharieh, A., M. Itriq and W. Dbabat, 2008. A dynamic resource synchronizer mutual exclusion algorithm for wired/wireless distributed systems. Am. J. Applied Sci., 5: 829-834. DOI: 10.3844/.2008.829.834