A Novel Method of Inconsistent Collision Detection to Prevent Cloning Attacks in High-Security Wireless Body Area Networks

Govindharajan Uma Gowri*[,1], Rajagopal Sivakumar[#2]

*Associate Professor and Head, Department of Electronics and Communication Engineering,
Madha Engineering College, Chennai, Tamil Nadu, India.
umagowri.g@gmail.com

[#]Professor and Head, Department of Electronics and Communication Engineering,
RMK Engineering College, Chennai, Tamil Nadu, India.

Abstract—Remote monitoring of physiological data of patient is emerging as technology called Wireless Body Area Networks (WBAN). As WBAN devices are operated in hostile environments, providing security and privacy to patients are challenging tasks. Due to simple, low cost and resource constrained nature of the sensors of WBAN, adversary can easily compromise one or more nodes and make clones of compromised nodes to launch different insider attacks in the network. In this paper, we propose a clone detection and prevention strategy for WBAN by leveraging inconsistent collisions so that legitimate nodes of WBAN are alone allowed to participate in communication, while preventing the cloned nodes. Through simulation, we show that the proposed algorithm can detect cloning attack fairly fast and with required accuracy under various conditions.

Keyword: WBAN, Security, Unreconciled collision, Cloning attack detection, Prevention

I. INTRODUCTION

A body area network is defined by IEEE 802.15.6 as "A communication standard optimized for low power devices and operate on, in or around the human body (but not limited to human) to serve a variety of applications including medical, consumer electronics/personal entertainment and other". A body area network is an interconnection of self configuring nodes attached to the surface, implanted in the body or embedded in the clothing for application in healthcare, sports, entertainment, military, pervasive computing and many other areas (1, 14, 17, 18). Sensors such as ECG electrodes, EEE electrodes activity sensors, temperature sensor, pulse rate sensors etc (22) along with memory and computational facility make the nodes of WBAN.

Technical advancement in the development of low power integrated circuits, ultra low power RF technologies, wireless communications and energy harvesting and storage has given birth to light weight, low cost, tiny and intelligent medical devices there by making pervasive wireless networks as reality in near future (9).

A WBAN is a wireless sensor network specifically deals with the challenges of monitoring human body as well as interaction of human body with environments. These challenges are different because of complex internal atmosphere of human body and individual attributes of human body that respond to and interact with outside world (14). Based on the devices, WBAN can be classified as Invasive WBAN and Non-Invasive WBAN. Invasive wireless body area networks supports in-body communication and the two-way communication between implanted medical devices and the external base stations and non invasive wireless body area networks support communication among non-invasive sensors on or close to the human body and the surrounding (11).

The fully functioning WBAN manages the communication of a set of heterogeneous nodes place on or inside the human body. Implanted nodes may operate within the Industrial Scientific Medical (ISM) Band at 2.4 GHz. Due to the low power and short range limitations of sensor nodes, a sink or BAN network controller (BNC) in the form of a mobile phone or portable device would receive the sensor data from various nodes, perform the necessary local processing and act as a local gateway for further communication over, eg., WiFi or General Packet Radio Services (GPRS) to a remote server for further processing and monitoring. Fig.1 shows a typical WBAN architecture where the PDA acts as the BNC to manage the data communication to the secure medical server through Wi-Fi, GPRS and the internet (16).

Using WBAN, a wide range of novel applications can be enabled such as Ubiquitous Health Monitoring (UHM), computer assisted rehabilitation, Emergency Medical Response System (EMRA) and for promoting healthy life styles. In VHM, the WBAN free people from visiting the hospital frequently and eases

the heavy dependence of work force in heath care. It can build cost effective health care systems for countries that are short of medical infrastructure and well trained staff. In an EMRS, temporary WBANs can be rapidly deployed with minimum workforce at a disaster scene so that vital signs of injured patients can be monitored and immediately reported to the remote health centre in time thereby saving the lives of many people.

II. WBAN SECURITY REQUIREMENTS

The security requirements of WBAN are data confidentiality, data authentication, data integrity, data freshness, secure management and availability. Data confidentiality is required to protect data from disclosure. Data authentication is required for each BAN Node (BN) and WBAN Network Controller (BNC) to verify that the data was sent by authorized sensor and not by an adversary. Data integrity enables sensor nodes to detect modified or injected packets. Data freshness ensures that the data is fresh and in order and are not replayed packed. Secure management is required at the BNC as it provides key distribution to the BNs for encryption and decryption operation also for secure association and disassociation of BNs with BNCs. Availability ensures that the patient's information is always availability to the physician for its intended use (26).

III. SECURITY THREATS

A simple design and limited capacity of sensor nodes make sensor networks prone to different types of attacks (13, 19, 20, 23, 28). Threats in WBAN can be classified as outsider attack and insider attacks. In an outsider attack, the advisory node is not an authorized participant of the sensor network. Authentication and encryption techniques prevent an outsider attacker to gain any special access to the WBAN. The intruder can only launch passive attacks like: (i) passive eavesdropping where the attacker eavesdrops and records encrypted messages, and then analyze to discover secret keys, (ii) Denial of service attacks, where adversary attempts to disrupt the network operation by broadcasting high energy signals and jamming the communication between legitimate nodes and (iii) Replay attacks, where the attacker captures the messages exchanged between legitimate nodes and replays them in order to change the aggregation result (15).

Due to simple and low cost sensor nodes, WBAN can be affected by a very dangerous and important insider physical attack called cloning attack or node replication attack. In this attack, the adversary physically captures one or few legitimate nodes, reads the secret credentials of compromise node, clones or replicates them with the same identity and finally deploys a capricious number of clones throughout the network (7, 21, 24, 30, 32). Using these clones, the attacker can launch several kinds of attack without being easily detected: (i) unauthorized access to health data, (ii) false data injection, where the attacker injects false results which are different from true health data sensed by bio-sensors, (iii) selective reporting where the attacker changes the reports of events by dropping legitimate packets that passes through the compromised node and (iv) alteration of health data of a patient, thereby needing to incorrect diagnosis and treatment (10). If these replicated nodes or clones remain undetected or unattended for a long time, they can further make changes in protocol behavior and intrusion into the system security (15). As clone attackers are severely destructive, effective and efficient solution for clone attack detection are needed to limit their damage. Several clone node detection schemes have been proposed to detect such attacks however; these solutions are not suitable because they demand in terms of energy, memory and execution time. We propose a protocol to detect and prevent cloning attack with fairly fast with required accuracy.

The rest of this paper is organized as follows: Section IV discusses the most related work on Clone attack detection, Section V presents WBAN threat environment model, Section VI deals the preliminaries and our scheme on detection and prevention of clone attacks, Section VII presents security analysis and performance evaluation and finally we conclude this paper in Section VIII.

IV. RELATED WORKS

The first solution for the detection of clone attacks depends on centralized Base Station (BS) (12). In this, each node sends a list of its neighbors and its location claims i.e, the geographical coordinates of each node to the BS. The same ID with inconsistent location in two list will detect clone nodes and BS revokes the clones. The drawback of this solution is the presence of single point failure (the BS) and high communication cost due to higher number of messages exchanged. Also, nodes close to BS will require routing many more messages than other node there by reducing their operational life time.

Brooks et al., (4) proposed another solution where a random key pre distribution security scheme is implemented in the sensor network. In this, each sensor node is allocated a set of k symmetric keys, randomly selected from a larger pool of keys. To detect, each node constructs a counting bloom filter from the keys it uses for communication. Then each node sends its own filter to the Base Station. The BS collects all reports from sensors and counts the number of time each key is used in the network. Often used keys (above threshold) are considered as cloned and a corresponding revocation procedure is executed.

To address node replication attack, Parno *et al*., (24) proposed two protocols: Randomized multicast and Line-Selected Multicast. In randomized multicast, each sensor node broadcasts a location claim to its neighbors. Each neighbor selects some random location within the network and forwards the location claim to

randomly selected nodes as witness nodes, exploiting the birthday paradox to detect clone nodes because at least one witness node is likely to receive conflicting location claims when cloned nodes exist in the network. Line selected multicast scheme uses the topology of the network to improve detection. In addition to witness nodes, the nodes along the multicast path also check the node clone. To increase the detection probability in both the schemes, nodes have to buffer more messages and require high communication cost. To choose random witness nodes, the schemes expect that every node is aware of all other nodes' presence, which is a very strong assumption for large scale sensor networks thereby limiting their applicability.

Zhu *et al*., (31) proposed two more efficient distributed protocols for detecting node replication attacks: single Deterministic Cell (SDC) and Parallel Multiple Probabilistic Cells (P-MPC). Both protocols require the sensor network to be a geographic grid where each unit of grid is referred as a cell. In SDC each node's ID is uniquely mapped to one of the cells in the grid. During execution of detection procedure, each node broadcasts a location claim to its neighbors. Then each neighbor forwards the location claim with a probability to a unique cell by executing a geographic hash function with the input of the node's ID. Each node in the destination cell stores the location claim with a probability. So the clone nodes will be detected with a certain probability as the location claims of cloned nodes also will be forwarded to the same cell. P-MPC protocol differs in the number of destination cell with SDC where location claim is forwarded to multiple deterministic cells with various probabilities by executing a geographic hash function with the input of the nodes ID. Therefore, the clone nodes will be detected with a certain probability.

Bekara and Laurent-Maknavicius, (3) also proposed a new protocol for securing WSN against node replication attacks by limiting the order of deployment. This scheme implies sensors to be deployed progressively in successive generations. In this, only newly deployed nodes are able to establish pair wise keys with their neighbors and all nodes in the network knows the number of highest deployed generation. Therefore, the cloned nodes will fail to establish pair-wise keys with their neighbors because the cloned nodes belong to an older deployed generation.

Choi *et al*., (5) proposed a clone detection procedure in sensor networks called SET, where the network is randomly divided into exclusive subsets. Each subset is assigned a subset leader and members are one-hop away from their subset leader. Then, multiple roots are randomly decided to construct multiple sub-trees and each subset is a node of the sub-tree. Each subset leader aggregates member information and forwards to the root of the sub-tree. On each root of the sub-tree, the intersection operation is performed to detect replicated nodes. If the intersection of all subsets of a sub-tree is empty, no clone nodes exist in the sub-tree. In the final stage, each root forwards its report to the BS. The BS computes the intersection of any two received sub-trees to detect the clone nodes. Therefore SET detects clone nodes by sending node's information to the BS from subset leader to the root node of a randomly constructed sub-tree and then to the BS.

Real time detection of clone attack in WSN was proposed by Xing *et al*., (29) in which, each sensor computes a finger print by including the neighborhood information through a superimposed S-disjunct code. Each node stores the finger print of all neighbor nodes. Whenever a node sends a message, the finger print also included in the message and thus the neighbors can verify the fingerprint. The clone nodes will be detected and dropped since the finger print generated by cloned nodes may not match the same community as their locations of deployments vary.

A recent work for detection of node clone attacks in WSN was proposed by Conti et al (7, 8) called Randomized, Efficient and Distributed Protocol (RED) based distributed detection. In this protocol, the BS broadcasts a random value to all nodes in the network. In RED, the witness nodes are selected based on pseudo random function with the inputs of the node's ID, random value which is broadcasted by the BS and the number of destination locations. The operations of RED protocol are similar to the Parno *et al*. scheme except for the selection of witness nodes. Location claims with the same node ID will be forwarded to the same witness nodes in each detection phase. Therefore the replicated nodes will be detected in each detection phase. In every detection phase of RED, the witness node will be different as the random value broadcasted by the BS will be changed.

Anandkumar and Jayakumar (2) proposed the improved version of RED protocol called as SRED – Secure RED. When the cloned node tries to enter through another node into the network, it checks whether a similar kind of node is available already or not with the access pointer by verifying the ID. If it exists, then it runs the algorithm to find and compare the location of both similar networks with the Message Information Table (MIS) available. Based on previous history available in the same node with respect to past time periods t-1, t-2, t-3,… t-n, comparison of location is done and with this knowledge the verifying node concludes whether the node is original or the duplicated node. Then the duplicated node is automatically revoked from the network and communication from that node is completely discarded by other nodes. This preliminary detection method reduces energy cost and communication overhead compared to other methods.

V. THREAT ENVIRONMENT MODEL

A. Network model

We consider a hospital scenario as shown in Fig.2, where there are many wards and patients in each bed of ward are fixed with set of sensors called as BAN Nodes (BNs) on their body to form wireless body area network. Patient may have BNs collect physiological information of patients and forwards to the BAN Controller (BNC) which may be a PDA or special device capable of collecting data from different BNs fixed on the patient, process and forward the aggregated data to the local CCU fixed at every ward. The main CCU or access point of the hospital gathers all information from various local CCUs and forwards the data to the doctor for required diagnosis and prescription or to the nursing station for required assistance.

We assume a simple yet powerful adversary. The adversary would be in and around the hospital environment so that he comes in the range of communication with the particular local CCU or access point near to the ward. The adversary can compromise a fixed amount of nodes with the help of sniffing tools by monitoring the network movement. He then gets the cryptographic credentials of the compromised nodes and makes one or more replicas of compromised nodes to insert into the network. These cloned nodes may compromise or fully control the network operation by injecting false data into the network or disturbing local control protocols such as localization, time synchronization and route discovery process. It can also launch denial-of-service attacks by jamming the signals from legitimate nodes. In general, to cope with this threat, it could be possible to assure that the nodes are tamper proof. We also assume that the patients are stationary and there are no cloned nodes at the time of initialization.

VI. PRELIMINARIES AND DETECTION ALGORITHM

A. Reconciled and unreconciled collision in WBAN

To implement our design, we expect the nodes to decide when to respond according to their IDs such that nodes with the same ID always simultaneously respond and nodes with different ID could respond either simultaneously or asynchronously. When nodes with different ID respond simultaneously and cause collision then it is called as reconciled collision because this collision can be reconciled again by arbitrating access to the channel among them. On the other hand, collision due to response from nodes with same ID is referred as unreconciled collision and this type of collision cannot be reconciled by arbitrating channel access among the nodes. Intitutively, these unreconciled collision is probably due to the legitimate nodes and its cloned peers responding simultaneously with same ID in a same time slot. Therefore, determining unreconciled collision can uncover cloning attack in WBAN. To arbitrate channel access among nodes and to detect cloning attack, any one collision arbitrating protocol can be used. We propose to use framed Aloha for our design to detect cloning attack (25).

Fig.3. shows the sample of six nodes N_1 to N_5 with IDs id1 to id5 and in which id4 corresponds to a legitimate node n4 and its cloned node. In the first frame with frame size F and random seed r_s, nodes respond in a time slot with index given by hash function $h(F, r_s, ID)$. The nodes N_1 and N_5 respond in two different singleton slots, where as N_2 and N_3 respond in the same timeslot referred as first collision slot and the legitimate N_4 and its clone with same ID respond simultaneously in the same time slot giving second collision slot. To reconcile the first collision, nodes N_2 and N_3 are allowed to respond again in the second frame with frame size F_1 and random seed r_{s1} and reconciling is done successfully because no collision occurs in the second frame. But using this reframing, second collision cannot be reconciled because nodes with same ID will select the same time slot while responding in the third frame with frame size F_2 and random seed r_{s2} making collision again. Using this procedure, unreconciled collision can be leveraged to detect cloning attack with higher probability.

B. Detection algorithm

In this section, we propose the enhanced collision slot reframing detection protocol against cloning attack to detect as well as prevent cloning attack in wireless body area network. This algorithm detects a cloning attack in WBAN if an unreconciled collision occurs. The protocol reconciles collision to find unreconciled collision in a voracious manner: After reconciling a collision, if some singleton slot(s) and some collision slot(s) are obtained, then protocol continues to reconcile the newly obtained collision(s). It reconciles collisions using collision slot reframing which an adaptation is of framed ALOHA. To reframe collision the nodes required to choose the slot to further respond in a new frame as shown in Fig.3. In the new frame if only one slot is collision and the others are empty, it finds an unreconciled collision and detects a cloning attack.

During collision slot reframing when the first non-empty slot in collision, then reframing is done only if it is followed by some non-empty slot(s). If collision slot is followed by only some empty slot(s) or by no slot, collision slot is not reframed, because the collision slot exposes an unreconciled collision. To determine whether or not to reframe the collision slot, the number of non-empty slots in the new frame is determined using

1 bit response. If the new frame has only one non-empty slot, only one collision slot will be contained under to bit responses which are the condition for an unreliable collision. If the new frame contains multiple non-empty slots, collision slot is reframed.

In our design, CCU first broadcast a query message indicating frame size F and random seed r_s. The sensor nodes in the time slot will index $h(F, r_s, ID)$ upon receiving the query message. The hash function $h(.)$ implemented on sensor nodes enables a sensor node to select in which time slot to respond uniformly at random. The response is a 10 bit string with CRC embedded for the CCU to verify collision. Upon determining an empty slot or a singleton slot, the CCU issues slot end command to initiate the next time slot. If it is a collision slot with a new frame size F_r and a new random seed r_{sr}, requiring 1-bit response to find out quickly the number of non- empty slots. If the new frame contains only one non-empty slot, then the algorithm decides it as an unreconciled collision, calculates the Gamma factor and stores in the Gamma table. In this way, it detects a cloning attack. In the next iteration, if the responding node id presents in the gamma table, it discards the communication of the node and revokes them from further process. Otherwise if CCU finds the second non-empty slot, it reframes the collision slot again with F_r and r_{sr} requiring 10 bit responses. Likewise, the CCU greedily reframes a collision slot whenever it verifies one. In a given F_r slotted frame, it verifies all non-empty slots and reframes collision slot if any, the CCU traces back to the collision slot it just frames and issues a slot end command to initiate the following time slot. Fig.4. illustrates the flow chart of a protocol execution instance.

VII. SECURITY ANALYSES

In this section, we investigate the effect of various parameters affecting our cloning detection protocol. Whenever the CCU requires the information from node, it broadcasts a frame F having N number of time slots in the frame. Each node sends request to the CCU at a particular instant of time and for each request a time slot is allocated to the node for transmitting data. During this process the time allocation, any tow of the nodes can send request at the same instant of time, thus occupying the same time slot which is called a s collision. After time slot allocation each node is allowed to transmit data to the CCU.

We analyze the maximum number M_s of slots in the f-slotted frame that the collision detection protocol needs to verify to satisfy a false negative rate α using established literature. For the given frame size F made available by the CCU, the tolerance number k of cloned IDs, the maximum number M_s of slots occupied by the response of the nodes in the F slotted frame, our protocol verifies to satisfy a false negative α is given by

$$M_s = \left[\left(1 - \alpha^{\frac{1}{k+1}}\right) F\right] \quad (1)$$

The above M_s is responsible for deciding how many nodes can be accommodated for transmitting data to the CCU.

When a collision is encountered in a particular time slot, reframing of time slot takes place. Given an unreconciled collision, the minimum reframing size $F_{r\min}$ requested to satisfy a required false positive rate β is given as

$$F_{r\,min} = \left[\beta^{\frac{1}{2}}\right] \quad (2)$$

Given the ID conditionality N, the tolerance number k of cloned IDs and the frame size F to satisfy a false negative rate α and a false positive β, the time taken to execute the process of detecting a cloned node is given as;

$$E[T(N,F,k,\alpha,\beta)] \leq \left[\frac{NM_sF_{r\,min}}{F}\right] t_s + \left[\frac{NM_sF_{r\,min}}{F} + M_s\right] t_c \quad (3)$$

where

$M_s = \left[\left(1 - \alpha^{\frac{1}{k+1}}\right) F\right]$, $F_{r\,min} = \left[\beta^{\frac{1}{2}}\right]$ denotes the time to detect an empty slot and $t_c = 2t_e$ is the time to detect a singleton or collision slot. The values of t_e and t_c are taken from the data sheet of biometric sensors whose frame size is given as f=22.7 sec and the time required for detection of an empty time slot is given as t_e =3360 ms. As $F = Nt_e$, using the typical values of F and t_e, the number of optimum slot per frame is approximately 7.

Thus there are seven slots available in a single frame sent by CCU. The number of nodes in a WBAN system is limited to 1000. This is due to the fact that the proposed system involves a hospital scenario, in which a group of CCUs can be coupled together to work in a cascaded manner so as to transmit large amount of patients data to the server. For each CCU there is given a maximum tolerance of 0.2 such that for 1000 nodes there can be a maximum of 200 cloned nodes for which our proposed system would detect clones with maximum probability whereas for more than 200 cloned nodes, the system is said to be inaccurate and leads to system failure.

A. Prevention ratio factor (γ)

A factor called as prevention ratio factor (γ) is proposed in order to reduce the effect of false negative rate (α) in the system. The gamma factor is given as;

$$M_s = \left[\left(1 - \alpha^{\frac{\gamma}{k+1}}\right) F\right] \quad (4)$$

When a collision slot is encountered in the CCU, an iterative process starts to identify the gamma function. The prevention ratio factor is selected according to the number of cloned nodes identified during the detection process when a node is identified as cloned in nature; the node is stored in a separate table as gamma table. In the next iteration, again a frame is sent by CCU and the response from the nodes is checked with the values in gamma table. If the collision slot node value matches with that of the node value in gamma table these the node is discarded for all the upcoming iterations for the number of cloned nodes stored in the gamma table a specific gamma value is calculated as

$$\gamma = N_c t_c + t_e \quad (5)$$

where N_c is the number of collision slots identified and γ is in the prevention factor ratio which is sent to CCU for the reframing command.

VIII. PERFORMANCE EVALUATIONS

In this section, we evaluate the performance of our algorithm through simulations. Simulations results show that our algorithm can detect as well as protect cloning attack in wireless body area network fairly fast with good accuracy.

A. Varying frame size (F)

We first analyze the impact of frame size F on the execution time of our algorithm. Fig.5 shows the results of execution time with and without prevention factor condition with false negative rate α=0.111, false positive rate β=0.111, k+1=1 cloned IDs, ID cardinality N=200 to 1000. Given a certain n and number of collision slots N_c, execution time of one algorithm is not a monotonically increasing function of F. As F increases first the execution time decreases and then increases giving minimum at F = 6 N. These variations of execution time are due to the variation of number of empty, singleton and collision slot. As F increases, the number of empty slots increases, the number of singleton slots increases up to N-(k+1) = N-1, while the collision slots decreases down to k+1=1. By our protocol design, collision slot reframing takes more time than an empty or a singleton slot. The execution time of our protocol decreases with the introduction of prevention factor γ. For each calculated values of prevention factor γ, the reduction in reframing time reduces the total number of slots occupied M_s, thus reducing the execution time required for the execution of algorithm.

B. Varying ID cardinality (N)

We also investigate the execution time of our algorithm in WBAN with varying ID cardinality N =200 to 1000 and is reported under conditions when frame size F =6N in Table 1 and 2. Table 1 gives the execution time with false negative rate α=0.111 and false positive rate β=0.111, number of collision slots N_c =150 and varying tolerance number k of cloned IDs. Given a fixed k, the execution time increases with N and given certain N, the execution time decreases with k. Table 2 reports the execution time with β=0.111, k=5, number of collision slots N_c =150 and varying α. Given a forced α, the execution time increases with N; given a certain N, the execution time decreases with α. The above procedure is repeated to see the change in execution time after including the prevention factor in our algorithm as shown in Tables 3 and 4.

In summary, (i) given certain α and k, the execution time increases with N; (ii) given a fixed N, higher α and k gives faster detection and (iii) inclusion of prevention factor (γ) reduces the execution time and makes detection and prevention faster.

IX. CONCLUSION

In this paper, we propose a cloning attack detection and prevention for wireless body area networks. The proposed protocol leverages the unreconciled collision to detect and also prevent cloning attack. Simulation results reports the protocol can detect cloning attacks in WBAN fairly fast with required accuracy. Our future work will explore other kinds of cloned detection mechanism in wireless body area networks.

ACKNOWLEDGEMENT

The authors are indebted to all the colleagues, especially those from the Department of Electronics and Communication Engineering, Madha Engineering College for their valuable suggestions on the manuscript and laboratory work.

REFERENCES

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: a survey," Computer Networks, vol. 38, pp. 393-422, 2002.
[2] K. M. Anandkumar, and C. Jayakumar, "Prevention of clone attacks in pervasive healthcare environments," Eur. J. Sci. Res., vol. 72, pp. 348-359, 2012.
[3] C. Bekara, and M. Laurent-Maknavicius, "A new protocol for securing wireless sensor networks against nodes replication attacks," in Proc. WiMob '07, 2007, pp. 59-65.
[4] R. Brooks, D. Y. Govindaraju, M. Pirretti, N. Vijaykrishnan, and M. T. Kandemir, "On the detection of clones in sensor networks," IEEE Trans. Syst. Man. Cybernetics, vol. 37, pp. 1246-1258, 2007.
[5] H. Choi, S. Zhu, and T. F. La Porta, "SET: Detecting node clones in sensor networks," in Proc. SecureComm '07, 2007, pp. 341-350.
[6] J.J. Clifton, Hazard prediction. In: Disaster prevention, planning and limitation. University of Bradford, Technical Communications Ltd, pp. 54-64, 1999.
[7] M. Conti, R. D. Pietro, L. V. Mancini, and A. Mei, "Distributed detection of clone attacks in wireless sensor networks," IEEE Transaction on Dependable Secure Computing, vol. 8, pp. 685-698, 2011.
[8] M. Conti, R. D. Pietro, and L. V. Mancini, "A randomized, efficient and distributed protocol for the detection of node replication attacks in wireless sensor networks," in Proc. MoblHoc'07, 2007, pp. 80-89.
[9] G. A. Conway, S. L. Cotton, and W. G. Scanlon, "An antennas and propagation approach to improve physical layer performance in wireless body area networks," IEEE Journal on Selected Area in Communications, vol. 27, pp. 27-36, 2009.
[10] T. Dimitriou, and K. Ioannis, "Security issues in biomedical wireless sensor networks," 1st International Symposium on Applied Sciences in Biomedical and Communication Technologies, 2008, pp. 1-5.
[11] S. Drude, "Requirements and application scenarios for body area networks," Mobile and Wireless Communications Summit, pp. 1-5, 2007.
[12] L. Eschenauer, and V. D. Gligor, "A key management scheme for distributed sensor networks," Proceedings of the 9th ACM Conference on Computer and Communication Security, 2002.
[13] Z. M. Fadlullah, M. Fouda, N. Kato, X. Shen, and Y. Nozaki, "An early warning system against malicious activities for smart grid communications," IEEE Network, vol. 25, pp.50-55, 2011.
[14] E. Farella, A. Pieracci, L. Benini, L. Rocchi, and A. Acquaviva, "Interfacing Human and computer with wireless body area sensor networks: the Wimoca solution," Multimed. Tools Appl., vol. 38, pp. 337-363, 2008.
[15] Gautam T.S. 2008. CINORA: Cell Based identification of node replication attack in wireless sensor networks, In Proceedings of the IEEE International Conference on Communication Systems-ICCS'08.
[16] L. Hughes, X. Wang, and T. Chen, "A review of protocol implementations and energy efficient cross-layer design for wireless body area networks," Sensors, vol. 12, pp. 14730-14773, 2012.
[17] A. Liu, J. Ren, X. Li, Z. Chen, and X. Shen, "Design principles and improvement of cost function based energy aware routing algorithms for wireless sensor networks," Computer Networks, vol. 56, pp. 1951-1967, 2012.
[18] R. Lu, X. Li, X. Liang, X. Shen, and X. Lin, "GRS: The green, reliability, and security of emerging machine to machine communications," IEEE Communications Magazine, vol. 49, pp. 28-35, 2011.
[19] R. Lu, X. Lin, X. Liang, and X. Shen, "A dynamic privacy-preserving key management scheme for location based services in vanets," IEEE Transactions on Intelligent Transportation Systems, vol. 13, pp.127-139, 2012a.
[20] R. Lu, X. Lin, X. Liang, and X. Shen, "Pseudonym changing at social spots: An effective strategy for location privacy in vanets," IEEE Transactions on Vehicular Technology, vol. 61, pp. 86-96, 2012b.
[21] R. Lu, X. Lin, H. Zhu, X. Liang, and X. Shen, "Becan: A bandwidth efficient cooperative authentication scheme for filtering injected false data in wireless sensor networks," IEEE Transactions on Parallel and Distributed Systems, vol. 23, pp. 32-43, 2012c.
[22] L. Ming, W. Lou, and K. Ren, "Data security and privacy in wireless body area networks," IEEE Wireless Communications, vol. 17, pp. 51-58, 2010.
[23] P. Papadimitratos, J. Luo, and J. P. Hubaux, "A randomized countermeasure against parasitic adversaries in wireless sensor networks," IEEE Journal on Selected Areas in Communications, vol.28, pp.1036-1045, 2010.
[24] B. Parno, A. Perrig, and V. Gligor, "Distributed detection of node replication attacks in sensor networks," Proceedings of the IEEE Symposium on Security and Privacy, pp. 49-63, 2005.
[25] L. G. Roberts, "Aloha Packet System with and without slots and capture," ACM SIGCOMM Comput. Commun. Rev., vol. 5, pp. 28-42, 1975.
[26] S. Saleem, S. Ullah, and K. S. Kwak, "Towards security issues and solutions in wireless body area networks," in Proc. INC, 2010, pp. 1-4.
[27] A. R. Sepaskhah, and M.M. Ghasemi, Every-other-furrow irrigation with different irrigation intervals for grain sorghum. Pak. J. Biol. Sci., vol.11, pp. 1234-1239, 2008.
[28] T. Shu, M. Krunz, and S. Liu, "Secure data collection in wireless sensor networks using randomized dispersive routes," IEEE Transactions on Mobile Computing, vol. 9, pp. 941-954, 2010.
[29] K. Xing, F. Liu, X. Cheng, and D. H. C. Du, "Real-time detection of clone attacks in wireless sensor networks," in Proc. IEEE International 1st Conference on Distributed Computing Systems, 2008, pp. 3-10.
[30] Y. Zeng, J. Cao, S. Zhang, S. Guo, and L. Xie, "Random-walk based approach to detect clone attacks in wireless sensor networks," IEEE Journal on Selected Areas in Communications, vol. 28, pp. 677-691, 2010.
[31] B. Zhu, V. G. K. Addada, S. Setia, S. Jojodia, and S. Roy, "Efficient distributed detection of node replication attacks in sensor

networks," in Proc. Annual Computer Security Applications Conference, 2007, pp. 257-267.
[32] B. Zhu, S. Setia, S. Jajodia, S. Roy, and L. Wang, "Localized multicast: Efficient and distributed replica detection in large-scale sensor networks," IEEE Transactions on Mobile Computing, vol. 9, pp. 913-926, 2010.

List of Figure

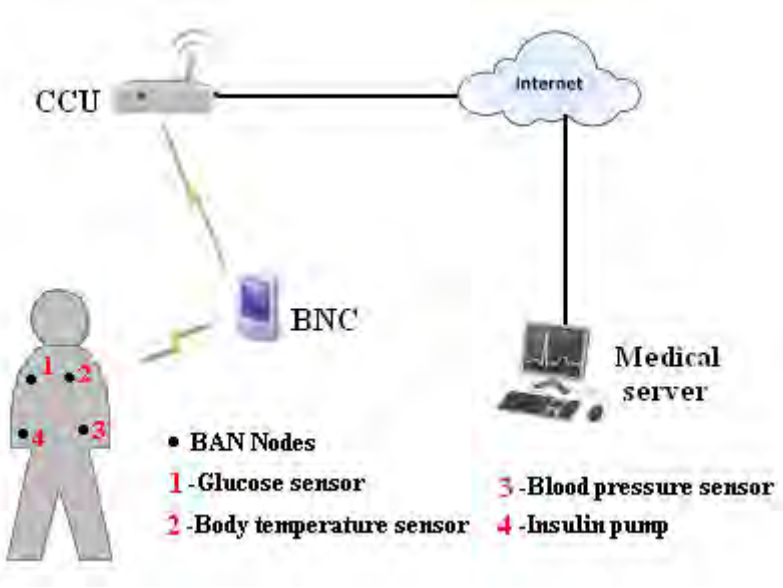

Fig.1. A typical BAN architecture

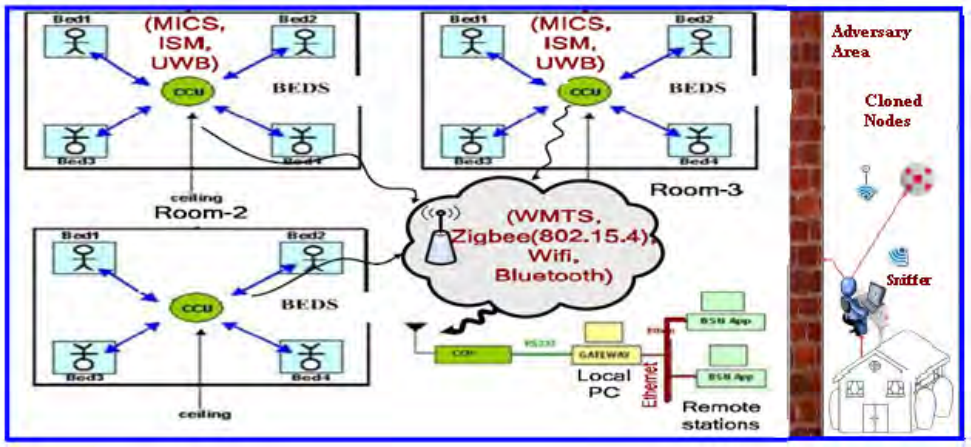

Fig.2. Network threat model with hospital scenario

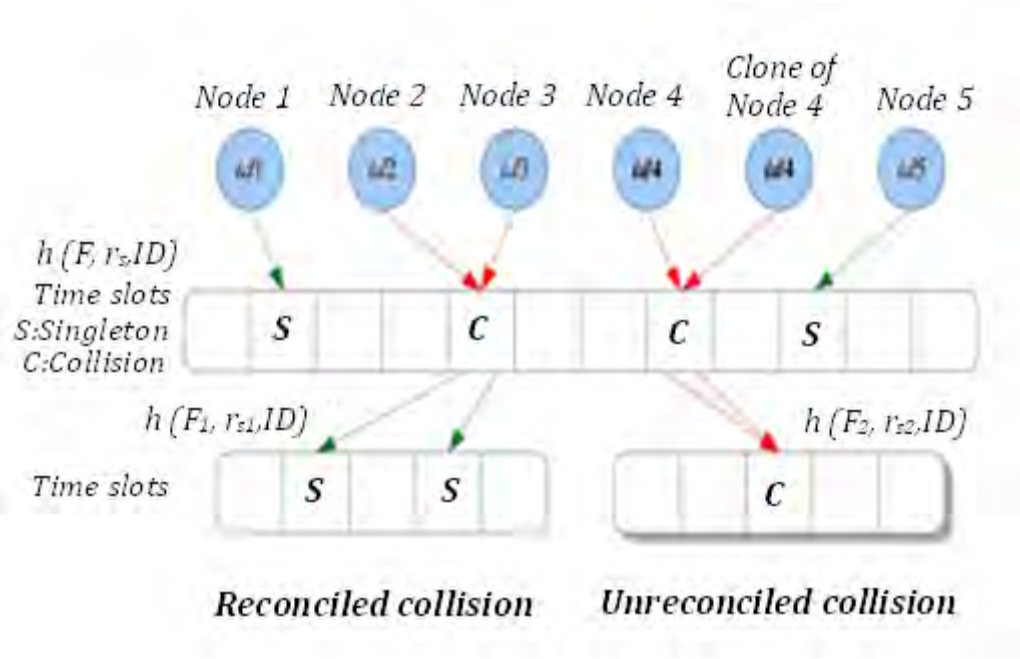

Fig.3. Example of an unreconciled collision due to response from two nodes with same ID

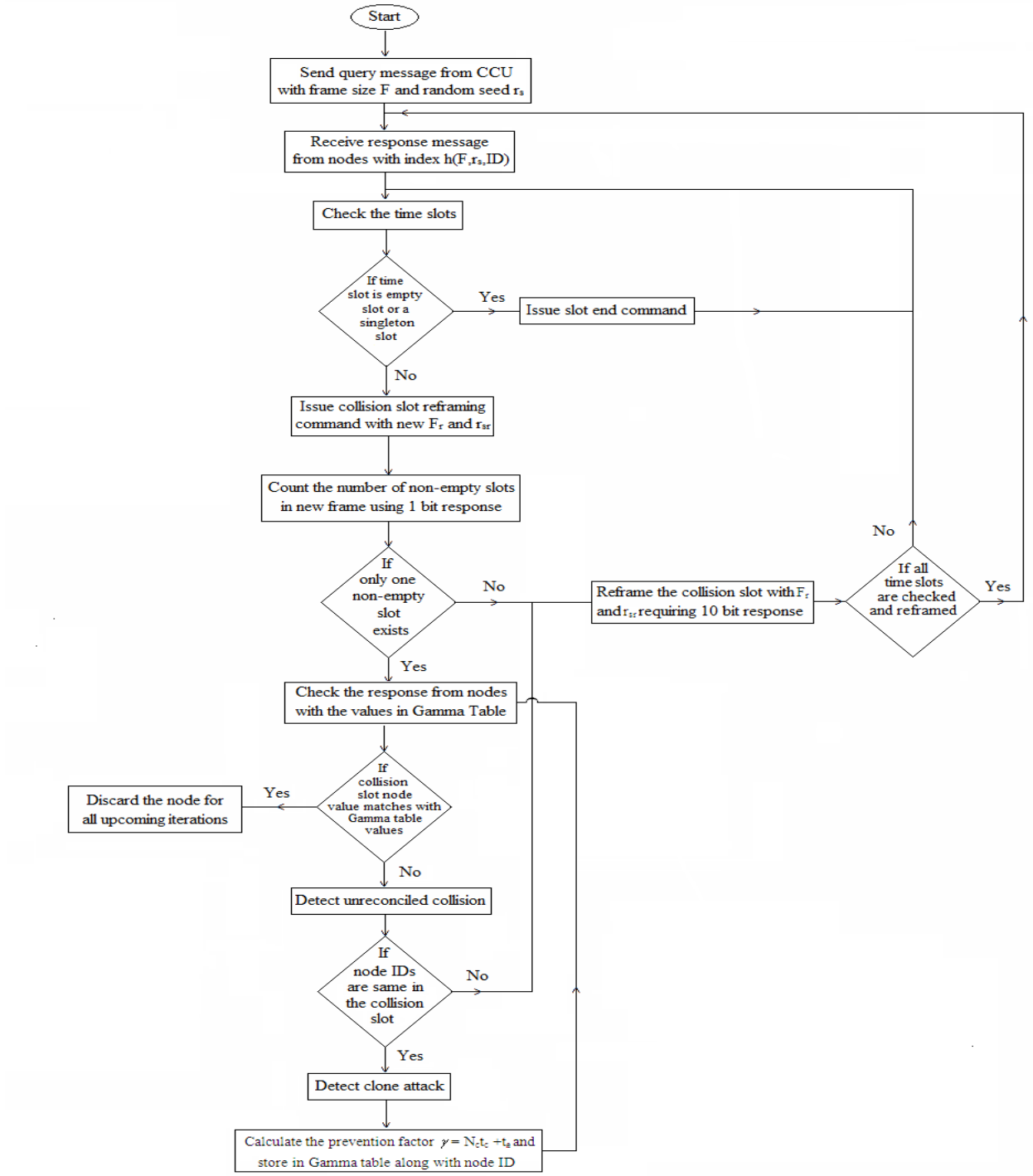

Fig.4. The flow chart of a protocol execution instance

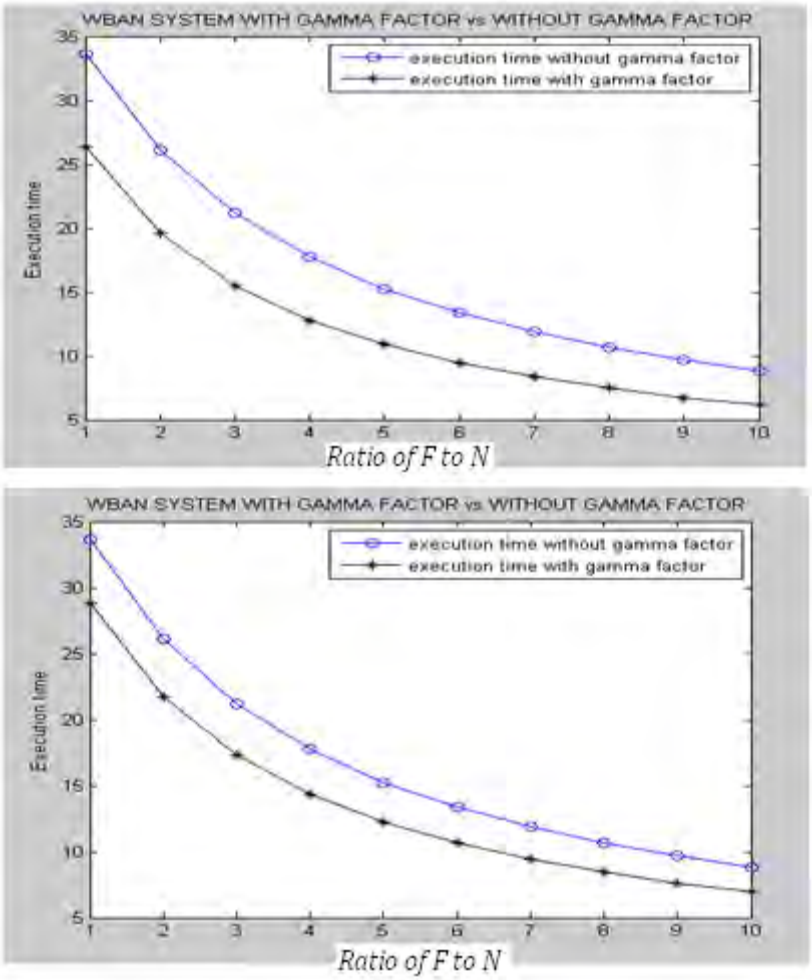

Fig.5. Execution time with varying frame size F under given ID cardinality N, tolerance number k of cloned IDs, false negative rate α, and false positive rate β (a) for N_c=160 and (b) for N_c=180

List of Tables

Table 1 Execution time with varying number of node *N*, varying tolerance number *k* of cloned IDs, frame Size $F = 6N$, false negative Rate $\alpha = 0.111$, false positive rate $\beta = 0.111$ and number of collision nodes N_c=150.

N	**Execution time (s)**			
	***k* = 2**	***k* = 4**	***k* = 6**	***k* = 8**
200	5.23	3.58	2.71	2.18
300	7.85	5.37	4.07	3.27
400	10.47	7.17	5.43	4.36
500	13.09	8.96	6.79	5.46
600	15.71	10.75	8.15	6.55
700	18.32	12.55	9.51	7.64
900	23.56	16.13	12.22	9.83
1000	26.18	17.93	13.58	10.92

Table 2 Execution time with varying number of nodes *N*, tolerance number *k*=5 of cloned Ids, frame size *F* =6*N*,varying false negative rate α, false positive rate β = 0.111 and number of collision nodes N_c=150.

N	**Execution time (s)**			
	***α*=0.112**	***α*= 0.115**	***α*=0.117**	***α*=0.12**
200	3.0823	3.0514	3.0312	3.0013
300	4.6234	4.5771	4.5467	4.5020
400	6.1646	6.1028	6.0623	6.0027
500	7.7057	7.6285	7.5779	7.5033
600	12.35	12.22	12.13	12.01
700	9.2469	9.1542	9.0935	9.0040
900	13.8703	13.7312	13.6402	13.5060
1000	15.4115	15.2569	15.1558	15.0067

Table 3 Execution time with varying number of node *N*, varying tolerance number *k*, frame size *F* =6*N*, false negative rate α = 0.111, false positive rate β= 0.111, number of collision nodes N_c=150 and prevention ratio factor γ

N	**Execution time (s)**			
	***k* = 2**	***k* = 4**	***k* = 6**	***k* = 8**
200	4.14	2.74	2.04	1.63
300	6.21	4.11	3.06	2.44
400	8.28	5.48	4.09	3.26
500	10.35	6.85	5.11	4.07
600	12.43	8.23	6.13	4.89
700	14.50	9.60	7.16	5.70
900	18.64	12.34	9.20	7.33
1000	20.71	13.71	10.23	8.15

Table 4 Execution time with varying number of nodes *N*, tolerance number *k*=5 of cloned IDs, frame size *F* =6*N*,varying false negative rate α, and false positive rate β= 0.111, number of collision nodes N_c=150 and prevention ratio factor γ

N	**Execution time (s)**			
	***α*=0.112**	***α*= 0.115**	***α*=0.117**	***α*=0.12**
200	2.3361	2.3114	2.2953	2.2715
300	3.5042	3.4672	3.4429	3.4073
400	4.6723	4.6229	4.5906	4.5430
500	5.8403	5.7786	5.7382	5.6788
600	7.0084	6.9343	6.8859	6.8145
700	13.01	12.87	12.79	12.66
900	10.5126	10.4015	10.3288	10.2218
1000	11.6806	11.5572	11.4764	11.4764