International Journal of Security and Its Applications
Vol.8, No.5 (2014), pp.457-470
http://dx.doi.org/10.14257/ijsia.2014.8.5.39

The Research of Secure Transport Protocol Based on Node's Clock Characteristics for Body Area Networks

Tan Jin[1, a] and Wang Yijing[2, b]

([1,2]*Information College, China Ji Liang University, Hangzhou, 310018, China*)
[a]*tanjin@cjlu.edu.cn*, [b]*wyj9068@163.com*

Abstract

The data security and privacy are key issues, as well as the security measures of clinical application are desired to be simple operations of "plug and play" for wireless body area networks (BAN). In this paper, a secure multi-hop data transmission protocol based on combination of node's clock characteristics and properties of the BAN/BSN is presented without relying on any pre-distributed secret information. First, through exchanging clock frequency (CF) among node x, its neighbor i and sink in a safe environment, the pair-wise K_x between node x and sink is generated with CF of x and is used to encrypt data sensed by x; the pair-wise K_{xi} or K_{ix} between x and i is generated with clock skew of two nodes is used to encrypt route information; Second, the RREQ and RREP messages of AODV protocol is improved, and creates a secure route only composed of legal nodes through authenticating nodes with CFs of two adjacent nodes; Finally, the data packet produced by source x is divided into Data1 and Data2, Data2 is the being sensed data encrypted with K_x, and Data1 encrypted with K_{xi} or K_{ix} includes source, destination, generated time of data and other information, the intermediate node needs to encrypt Data1again after decrypting Data1 to obtain route information, and transmits this data packet to sink with hop-by-hop. This protocol has good security in dynamics and accuracy of keys, avoiding passive and active attacks, preventing node capture and supporting new node joining through security analysis, and has accepted overheads of memory, computation and energy consumption by means of performance analysis; it satisfies the requirements of "plug and play" without added node's hardware and pre-load any keys, makes the complicated data security and privacy in the BAN/BSN become operable easily and practicable strongly.

Key Words: *Body Area Networks; Clock Skew; Symmetric Key; Secure Protocol*

1. Introduction

Body area networks (BAN), also called Body sensor networks (BSN), consist of a certain number of physiological sensor nodes placed on the human body surface (some nodes may be implanted in body) and one gateway node (or sink) which transmits collected information from sensors to a base station, and are used for monitoring human physiological data in various healthcare applications [1]. Because the physiological and medical data sensed by sensors in a BAN/BSN play important roles in medical diagnosis and treatment, and involve privacy of the patient, so the data security and privacy is one of the key problems for the BAN/BSN [2]. In order for a patient to wear and move, the wireless channel is usually used for the data transmission between nodes in a BAN/BSN, especially multi-hop transmission in a BAN/BSN will be the main mode of communication in the future, this is because short

ISSN: 1738-9976 IJSIA

range transmission of ultra-low power is beneficial to human body [3], but it is critical to secure this data. There are many articles in which the security for general sensor network have been deeply researched in recent years [4-5], as a branch of WSN, the BAN/BSN has many similarities with WSN, but is different from WSN in deployment methods, node types and scales, date rate, latency and mobility. The biggest difference is that the general WSN is assumed to run at the unattended environment, whereas the BAN/BSN is under surveillance of the patient carrying these nodes or some medical personnel.

Information encryption and node authentication are the main measures to assure network security communication in WSN, the key management is a crucial part of security to ensure information confidentiality, integrity and prevent illegal node intrusion [6]. Because of high energy consumption and memory occupation, most public key techniques are still found to be unaffordable to biosensors of BAN/BSN, and are also considerably slow for encryption and decryption large volumes of health data in practice [7]; Especially this asymmetric cryptography is restricted in clinical application because of its dependence on the environment and the complexity of operation. In a traditional WSN, the information encryption and node authentication are partly ensured through pre-loading or pre-distributing various keys, such as master key, pair-wise key and number random keys chosen from much larger pool of keys generated offline [4]. If a WSN has N nodes and each node is pre-distributed N-1 pair-wise keys, a unique pair-wise key between each pair of sensor nodes is used to provide node-to-node authentications; the security of data transmission is ensured [4]. The main drawback of this solution is the great memory overhead it produces when N is larger, since each node have to store many keys may never be used. In a BAN/BSN, this solution may be used because N is smaller, but it has three shortcomings obviously besides not preventing node capture attack, is not suitable for a BAN/BSN in fact. (1) Each BAN/BSN must be pre-distributed N pair-wise keys (each node is pre-distributed N-1 keys) completely different from others, otherwise a pair-wise key between two nodes in respective BAN/BSN may be formed and results in error transmission when two patients get close, this increases the difficulty and complexity of pre-distributing keys. (2) Because the nodes in a BAN/BSN are heterogeneous, and may be come from different manufacturers; due to the lack of professional knowledge about security, end users are more hoping to operate it "plug and play" simply rather than to master prior security context among nodes when a BAN/BSN is used at begin; any key distribution/management process in a BAN/BSN should be minimized, automatic, and transparent to users in clinical care [8]. (3) It is very difficult to change the keys in the network which have been compromised [9].

The physiological information, such as PV (physiological value-based)[9], ECG (electrocardiogram) [10, 11], and PPG (photoplethysmogram) [12], are used to authenticate nodes and information in most existing studies as a secret channel; these solutions can achieve the "plug and play" effect without prior shared secret keys, but have a great demand on the capabilities of hardware and software of nodes; that is to say these require all nodes to be equipped with specific hardware and software to sense same physiological signal [13]; moreover, it is hard for every sensor in different positions of the patient to measure the same physiological signal with the same accuracy [8]. Using the channel characteristics of BAN/BSN, such as RSS (Received Signal Strength), is another research direction in generating a pair of symmetric keys, although the problems of accuracy of same physiological signal acquisition at different positions of the patient are avoided in these solutions, but the process of shared secret key generation is typically comprised of channel sensing, quantization, reconciliation and privacy amplification four phases [14], this leads to the low efficiency of key extraction.

The clock frequency (CF) of a node (defined in 4.1) is showed dynamic and uniqueness

achieved at each time; under control of sink, a pair-wise key is generated between two nodes through exchanging respective CF in a safe environment, this achieves the effects of preloading keys. In this paper, a secure multi-hop data transmission protocol based on combination of node's clock characteristics and properties of the BAN/BSN is presented without relying on any pre-distributed secret information. First, through exchanging CF among node x, its neighbor i and sink in a safe environment, the pair-wise K_x between node x and sink is generated with CF of x and is used to encrypt data sensed by x; the pair-wise K_{xi} or K_{ix} between x and i is generated with clock skew of two nodes is used to encrypt route information. Secondly, the *RREQ* and *RREP* messages of AODV protocol is improved, which creates a secure route only composed of legal nodes through authenticating nodes with CFs of two adjacent nodes. Finally, the data packet produced by source x is divided into Data1 and Data2, Data2 is the being sensed data encrypted with K_x, and Data1 encrypted with K_{xi} or K_{ix} includes source, destination, generated time of data and other information, the intermediate node needs to encrypt Data1again after decrypting Data1 to obtain route information, and transmits this data packet to sink with hop-by-hop. This protocol has good security in dynamics and accuracy of keys, avoiding passive and active attacks, preventing node capture and supporting new node joining through security analysis, and has accepted overheads of memory, computation and energy consumption by means of performance analysis; it satisfies the requirements of "plug and play" without added node's hardware and preload any keys, makes the complicated data security and privacy in the BAN/BSN become operable easily and practicable strongly.

The rest of this paper is organized as follows. We review related work in Section 2. The system model and attack model is introduced in Section 3. Section 4 presents our protocol based on the CF and clock skew, while Section 5 and Section 6 give security analysis and performance of our protocol. We conclude the paper in Section 7.

2. Related Works

The communication of the physiological and medical data between sensors in a BAN/BSN is subject to the following security requirements: confidentiality, authenticity, integrity and data freshness, design of security protocols in a BAN/BSN should be taken into account the particular attributes such as scale, heterogeneity of nodes and deploying on human body only [15]. Because key pre-distribution in a traditional WSN does not meet the "plug and play" requirements, the researches about communication of symmetric encryption in a BAN/BSN are more focused on using physiological information and wireless channel characteristics.

Because the physiological and medical data of patient are monitored in a BAN/BSN and the physiological signal is not easy to imitate, many biometrical values have been recently studied as a secure channel from which nodes can derive a common secret from a specific patient's body. Venkatasubramanian and Gupta [9] have presented a novel scheme for securing inter-sensor communication in a BAN/BSN called Physiological Value based Security (PVS), such as blood glucose, blood pressure and hemoglobin. Literature [10] presents an ECG-signal-based key establishment protocol to secure the communication between every sensor and the control unit, the confidentiality and integrity of the sensitive health information are protected; Zhang, Wang, *et al.*, [11] improve the Jules Sudan (IJS) algorithm to set up the key agreement for the message authentication, propose ECG-IJS key agreement that can secure data communications over BAN/BSN in a plug-and-play manner without any key distribution overheads through sharing a common key generated by ECG

signals; Literature [12] proposes a novel protocol, called Physiology-based End-to-End Security (PEES), which use ECG and PPG as a secure communication channel between the sensors and the back-end medical cloud in a transparent way, is light-weight for sensors because the strong and random keys are about 90 bits long only. Although the keys do not need to be pre-distributed in these solutions, but the same additional hardware is required for all sensors, and the accuracy of keys recovery cannot be guaranteed extractly [8].

In order to overcome the disadvantages of physiologic information as keys, the wireless fingerprints, such as signal strength, clock skew, frequency shift and transients [16], are used for node and message authentication in BAN/BSN in recent years [8, 17-18]. Shi and Li [8] propose a lightweight body area network authentication scheme (BANA) based on the distinct RSS variation behaviors between an on-body communication channel and an off-body channel, this means that the RSS variation of the channel between two legitimate nodes which are placed on the same user's body is much more stable than the case when one of the nodes is off-the-body, especially when the body as a whole is in motion. However, some sensor deployments are limited because BANA only considers authentication for LOS (line of sight) on-body nodes [17]; Literature [17] proposes a lightweight fast authenticated secret key extraction scheme for intra-BAN, which utilizes the relatively static channels for device authentication and the dynamic ones for secret key generation, and high secret key generation rate is achieved; Ali, Ostry, *et al.*, [18] propose a mechanism to secure data provenance for BAN/BSN by exploiting symmetric spatio-temporal characteristics of the wireless link between two communicating nodes, because the link fingerprints (RSS or signal phase) are very hard for an eavesdropper to forge, the accountability and non-repudiation of data can be provided. These solutions do not rely on key pre-distribution also, but the key extraction rate is limited by the wireless channel properties [13].

Clock skew is the inherent tiny drift in the clock of hardware devices due to variations in the manufacturing process, as a kind of fingerprint has been used for the 802.11 devices identification [19], time synchronization [20] and nodes identification [21-22] in a WSN. Furthermore, Literature [22] has showed that different nodes have different clock skew and nodes can be identified by their PPM (parts per million) level clock skew, and this clock skew can be used to identify virtual nodes on virtual honey-nets and malicious and malfunctioning node identification in WSNs, and to detect wormhole and sybil attacks as a fingerprint of wireless sensor nodes.

3. Network and Threat Models

3.1 Network Model

The network model of a BAN/BSN is depicted in Figure 1.

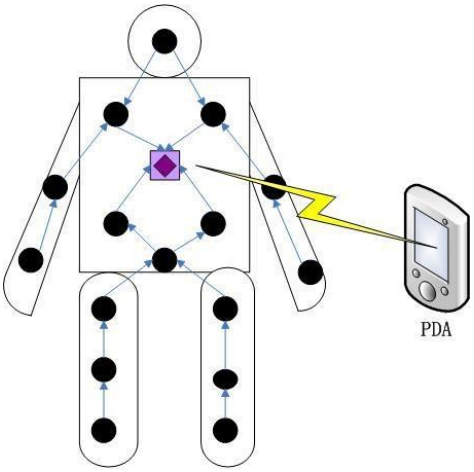

Figure 1. Network Model

(1) A BAN/BSN consists of a sink (gateway node) and a set of N sensor nodes $\{s_1, s_2, ..., s_{n-1}, s_N\}$ deployed on a body each with a unique ID (ID>0), all of them are equipped with the same wireless communication interface, such as ZigBee, and so is the sink;

(2) The sink (ID=0) is assumed to have abundant resources and varying power levels, these mean the sink can transmit message to all nodes of a BAN/BSN in single hop or multi-hop manner; As a controller, the sink is not compromised because it is physically protected or has tamper-robust hardware, and knows the running numbers and producing data frequencies of all sensors in its BAN/BSN;

(3) All nodes send their last sampled data to the sink in one (neighbor of sink) or more hops with ultra-low power, the data transmission protocol is assumed to be AODV [23];

(4) There are no malicious nodes and other BANs/BSNs around when a BAN/BSN is initialized (system initialization); this can be guaranteed in the indoor environment by the medical personnel or guardian operation;

(5) The BAN/BSN has taken some time synchronization, and this synchronization is safe, but the times of any two nodes are different at the PPM level.

3.2 Threat Model

The confidentiality and integrity of data are mainly considered in this paper, the threat model is assumed as follows:

(1) An adversary can easily eavesdrop message which sent by a sensor in wireless communication range, transmit this message after modification or delay at varying power levels;

(2) An adversary can masquerade as another legitimate node, and inject false data into the BAN/BSN;

(3) The denial of service (DoS) attack is not considered in this paper.

4. Protocol Descriptions

Our protocol has achieved "plug and play" effects without pre-distributing any key in nodes beforehand, and produces a pair-wise between two nodes with clock frequency and skew when the BAN/BSN is initialized, it is divided into three phases: system initialization, formation of secure routing and encrypted data transmission.

4.1 Clock Frequency and Skew

The clock frequency and skew are defined as follows [22]:

(1) Clock Frequency (CF): The rate at which a clock progresses, if $CF_x(t)$ is the time reported by the clock of node x at true time t, the clock frequency at t is denoted by $CF_x^{'}(t)$ (The frequency of true time is then 1):

$$CF_x^{'}(t) = dCF_x(t)/dt \qquad (t > 0) \tag{1}$$

(2) Clock Skew (CS): The difference in the frequencies of two clocks, the clock frequency between two nodes m and n at true time t is denoted by $CS_{mn}(t)$:

$$CS_{mn}(t) = CF_m^{'}(t) - CF_n^{'}(t) \qquad (t > 0) \tag{2}$$

Modern processor digital clocks have the following two properties generally [24]:

(1) The clock skew of any clock is stable under normal temperature;

(2) Every stable clock skew is considered unique and thus there exists a distinguishable relative clock skew between any two physical devices.

We use CF and CS to format secure routing and encrypt data as two fingerprints according to these two properties.

4.2 System Initialization

When a BAN/BSN powered on or reset, each sensor node clear all information in its memory, and transmits data to the sink with original AOVD protocol at this phase; the system initialization is performed in a secure environment as follows:

(1) The sink broadcast two time-stamps T_1, T_2 as true time at random intervals to all nodes in single hop manner;

(2) After T_1, T_2 are received by all nodes, node x $(1 \le x \le N)$ calculates its CF with $CF_x^{'}(T_2 - T_1) = (CF_x(T_2) - CF_x(T_1))/(T_2 - T_1)$, saves it in memory and sends it with node ID to the sink through original AODV; when the BAN/BSN started to work, node x encrypts its sensing data sent to sink with secret key:

$$K_x = F(CF_x^{'}(T_2 - T_1), ID_x) \tag{3}$$

Here F is a function to generate a secret key.

(3) When node x sends $CF_x^{'}(T_2 - T_1)$ with its ID to the sink, all the neighbors of node x (within one hop) receive it at the same time, and save it with its ID in respective memory, the CF+ID of other nodes will be received by node x; In this way, the CF exchanges are completed between two adjacent nodes in a BAN/BSN; When node x forwards CF+ID message of other nodes as an intermediate node, it does not need to store this message.

(4) In the path from node x to sink, two adjacent nodes m, n have each other's CF; the difference in the frequencies of two clocks of m and n is unique, and the $CS_{mn}(T_2 - T_1)$ can be used for the mutual authentication between nodes m and n at formation of secure routing or encrypted data transmission phase; the pair-wise key K_{mn} and K_{nm} are the same:

$$K_{mn} = K_{nm} = F(CS_{mn}(T_2 - T_1), ID_m, ID_n) \tag{4}$$

$$CS_{mn}(T_2 - T_1) = ABS(CF_m^{'}(T_2 - T_1) - CF_n^{'}(T_2 - T_1));$$

Here F is a function same as formula (3), and ABS represents the absolute value.

(5) After system initialization, the sink has saved the CFs of all nodes, and has a pair-wise key

K_x with node x; each node has saved the CFs of its neighbors, and two adjacent nodes m and n have a pair-wise key K_{mn} or K_{nm}; when sink broadcasts "OK" message in single hop manner, the BAN/BSN enters the formation of secure routing and encrypted data transmission phases.

4.3 Formation of Secure Routing

The pass loss rate of a BAN/BSN is higher than the general WSN due to the effect of the human body on propagation loss and link quality in various postures [4], the reactive protocol AODV is suitable for this situation which the connection is not stable and the forming route is the shortest; literature [25] has evaluated the performance of OLSR, AODV and DSR respectively with multiple BANs/BSNs in hospitals, and concluded that AODV is the best related to the others from delay, number of hops, throughput and packet loss point of view also.

When the "OK" message is received by all nodes, each node must delete the existed route (created in original AOVD) to sink in its memory at system initialization; when a node m want to send a message to the sink, it must reestablish the secure route to sink with added CF field in improved AODV protocol first, then transmits its data encrypted with K_m. The improved AODV protocol messages are presented in Figure 2; if a source node m $(1 \le m \le N)$ wants to send its data to the sink, the secure route from node m to sink is formatted as follows:

Tag	Source Address	Request ID	Source Sequence #	Destination Address	Destination Sequence #	CF	Hop Count

(a) RREQ

Tag	Source Address	Destination Address	Destination Sequence #	CF	Hop Count	Life Time

(b) RREP

Figure 2. Format of RREQ and RREP

(1) The source node m creates a *RREQ* message as Figure 1 (a), and fills the CF field of *RREQ* with its $CF_m^{'}(T_2 - T_1)$ first, then send *RREQ* message to all neighbors;

(2) When a neighbor node n $(1 \le n < N)$ receives the *RREQ* message from node m, it operates as follows:

A. If the CF field of *RREQ* is empty, the *RREQ* may come from a node cannot be trusted, it stops forwarding this message.

B. If the CF field exist and the $CF_m^{'}(T_2 - T_1)$ of node m saved in memory at system initialization is found, it compares $CF_m^{'}(T_2 - T_1)$ in memory to $CF_m^{'}(T_2 - T_1)$ in *RREQ*; if they are the same, it forwards *RREQ* after replacing $CF_m^{'}(T_2 - T_1)$ in *RREQ* with $CF_n^{'}(T_2 - T_1)$, otherwise stops forwarding this message (this shows that the *RREQ* is come from a faked node);

C. If the CF field exist and the $CF_m^{'}(T_2 - T_1)$ of node m is not found in its memory, this may be a consequence of changing network topology because of mobility or various postures of a patient, it may not has saved the clock frequency of node m $CF_m^{'}(T_2 - T_1)$ at system initialization. In such a case, it requests the $CF_m^{'}(T_2 - T_1)$ of node m from sink, the sink encrypts the $CF_m^{'}(T_2 - T_1)$ with K_n and sends it to node n in single hop manner; after the data

$CF_m^{'}(T_2 - T_1)$ is received by node n, it decrypts data with K_n and save the $CF_m^{'}(T_2 - T_1)$ in its memory, the subsequent operations are same with B;

(3) The neighbors of node n forward the *RREQ* message like step (2);

(4) The sink unicasts a route reply message (*RREP*) back to the source when the *RREQ* message is received, it creates a *RREP* message as Figure 1 (b), and fills the CF field of *RREP* with its CF (equal 1) first, then send *RREP* message back to its neighbor;

(5) When the neighbor of sink receives the *RREP* message, it send *RREP* message back to its neighbor like step (2);

(6) When the *RREP* message is received by source node m, the secure routing only composed of legitimate nodes is formed.

4.4 Encrypted Data Transmission

When the secure routing is formed, the source node can transmit data to the sink as show in Figure 3, the secure route from N1 to Sink is assumed to be N1-N2-N3-Sink;the node N1 is source and produces a data packet composed of Tag, Data1 and Data2; the tag is a message type, Data2 is sensing data, and Data1 includes source, destination, generated time of data and other information; in Figure 2, each node from N1 to sink operates as follows:

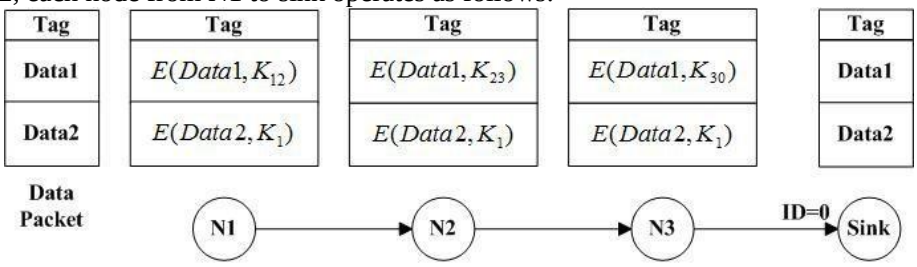

Figure 3. Encrypted Data Transmission

(1) Node N1: the $E(Data2, K_1)$ shows that Data2 is encrypted with K_1 known by N1 and sink only, the $E(Data1, K_{12})$ shows that Data1 is encrypted with K_{12} known by N1 and N2 only, and the data packet is sent to N2;

(2) Node N2: the Data1 is decrypted with K_{12} from $D(E(Data1, K_{12}), K_{12})$, the route information are obtained; the $E(Data1, K_{23})$ shows that Data1 is encrypted with K_{23} known by N2 and N3 only, and the data packet is sent to N3;

(3) Node N3: the Data1 is decrypted with K_{23} from $D(E(Data1, K_{23}), K_{23})$,the route information are obtained; the $E(Data1, K_{30})$ shows that Data1 is encrypted with K_{30} known by N3 and sink only, and the data packet is sent to sink;

(4) Sink: the Data1 is decrypted with K_{30} from $D(E(Data1, K_{30}), K_{30})$, the Data2 is decrypted with K_1 from $D(E(Data2, K_1), K_1)$.

Because the generated time of data is included in Data1 and the BAN/BSN has taken some time synchronization, the intermediate node N2 and N3 can determine whether the data packet from N1 is obsolete with a time threshold, and the sink can determine the validity of data from the interval of two values sensed by source node N1.

5. Security Analyses

Our proposed protocol does not require any prior distribution key, has ensured the

confidentiality and integrity of data in transmission, the security is analyzed from key dynamics and accuracy, active and passive attacks, node capture, new nodes joining and " plug and play" as follows:

5.1 Key Dynamics and Accuracy

The keys generated at each system initialization are dynamic; the intervals between T_1 and T_2 are random, the CF of each node and ID are unique, so the K_x calculated with formula (3) and K_{mn} calculated with formula (4) are dynamic. In addition, the values from formula (1) and (2) will change with various temperatures and different environments, these further increases the dynamics of keys.

Our protocol will not bring about the problem of accuracy of key recovery like extracting from physiological information, and also does not have the problem of low efficiency as extracting from wireless channel properties. Because the instant CF is calculated only once by the node itself without the need for a node to measure CF of another, and exchanged with other nodes in a safe environment; although it changes with various temperatures and different environments, but the instantaneous value of CF is achieved at system initialization, and used in formation of secure routing or encrypted data transmission, there is no key recovery process.

5.2 Passive Attacks

The malicious node can be infinitely close to the BAN/BSN, eavesdrops physiological data sent to sink by node x; because the physiological data (Data2) is encrypted with K_x and the route information (Data1) is encrypted with K_{xi} (node i is a next hop of x); the K_x can be calculated only by the CF and ID of node x obtained first from formula (3), the legitimate nodes in a secure route only know the data packet from which node, also do not know the contents of data; Even if the malicious knows the encryption function F when the BAN/BSN is working, but it neither know the data packet sent by which nodes, and do not know the data packet received by which the neighbor node. It is difficult to achieve the CF which was generated in system initialization and the ID which is in Data1 encrypted with K_{xj}, therefore it is difficult for the malicious to calculate K_x and decrypt the Data2.

5.3 Active Attacks

The four main forms of active attacks are replay, masquerade, modification and DOS, we consider the first three attacks only except DOS.

(1) Replay: it is meaningful only replaying obsolete data for an attacker, if a malicious node broadcasts an unmodified obsolete data packet as the node x, the neighbor i of x at the route from x to sink can decrypt $E(Data1, K_{xi})$ with K_{xi} and obtains route information from Data1 only, the node i may decide whether to forward this data packet according to the difference (time threshold) between its own time and generated time of data; even if the data packet is received by sink, it does not use this obsolete data according to the producing data frequency of x and alarms for help.

(2) Masquerade: the masquerade is that an attacker sends a fake data to the sink as a legitimate node; we assume that a malicious node has large enough power and all nodes in a BAN/BSN can receive this fake data:

A. When the malicious node forges a new node, the route form it to sink must be formed first, then the data can be transmitted. Because all sensor nodes and sink have no CF about the

malicious node, the secure routing is unable to establish with improved AODV protocol, so the fake data cannot be sent to the sink.

B. When the malicious node forges an existing legitimate node x, all neighbors of x can receive the fake data packet; the neighbor i tries to get route information from Data1 through decrypting $E(Data1, K_{xi})$ with K_{xi} $(1 \le i \le M, 1 \le M \le N)$, and stops forwarding the fake data packet due to the error in decrypting. Because the malicious is unable to obtain K_{xi}, node i cannot decrypt Data1 correctly, so the fake data cannot be sent to the sink.

(3) Modification: the modification is a kind of replay attack after the data is modified; this situation is illustrated with modifying Data2 (Data1 remains the same) of node x by the malicious node. The sensing data (Data2) is encrypted with K_x at the node x, and is sent to the neighbor of x with the Tag , Data1and Data2 as a data packet; the malicious node can receive this data packet and wants to broadcast the data packet again after modifying Data2 only, it must decrypt Data2 with K_x first, then modify the Data2 and encrypt the Data2 with K_x again; because K_x is known by x and sink only, the intermediate node does not verify the integrity of the Data2, the modified data packet can be transmitted to sink due to no change of routing information in Data1, but the integrity of the Data2 is destructed when the sink try to decrypted with K_x, the sink will discard this data packet and ask for help with alarm.

5.4 Node Capture

The node capture is that a legitimate node became malicious after it leaves the BAN/BSN for a period of time and then backs to; in this period, the attacker can obtain all information in a legitimate node, such as ID and CF of node, CFs of all neighbors and the key generation algorithm in function F; that is to say, the whole BAN/BSN is no secret because the K_x and K_{mn} are obtained easy through formula (3) and (4). In fact, the exclusion of a malicious node is relative easy in our protocol; First, the nodes in a BAN/BSN are heterogeneous and not related (each node senses data independently), when a node is in absence, the sink can find that a node is in failure or lost in a certain time range beyond the data interval of the absent node, ask for help with alarm; Secondly, because the BAN/BSN is under surveillance of patient and medical personnel or guardian, it is difficult for an attacker to physically access the nodes without this being detected for a long time [15], when a malicious is found, it is removed and the BAN/BSN is reset in a safe environment, this means that the new K_x and K_{mn} are generated in a new system initialization, when the another previous malicious node is entered the BAN/BSN again, it cannot initiate active and passive attacks because its K_x and K_{mn} are outdated.

5.5 New Nodes Joining and "Plug and Play"

When a new node is joined the BAN/BSN, the BAN/BSN is need to reset in a safe environment only; this means that system initialization, formation of secure routing and encrypted data transmission are performed again. The reset itself is a button operation and operable to medical personnel or guardian without professional knowledge, so the "plug and play" is achieved.

6. Performance Analyses

After the Second World War, the solution of protecting encryption algorithm is gave up,

and open encryption algorithm is adopted by increasing the key strength to achieve the purpose of confidentiality, such as AES [26] and PUFFIN [27]; our research focus is the data encryption transmission protocol under the strength of K_x and K_{mn} is met to requirements of security, the performance is analyzed from overheads of storage, computation and energy as follows:

6.1 Storage Overhead

In our Protocol, node x $(1 \le x \le N)$ has saved one own CF and M CFs and ID of neighbors in its memory; the K_x and K_{xi} $(1 \le i \le M)$ are calculated with formula (3) and (4), does dot occupy a fixed storage space; General the length of a CF (microsecond) is 4 bytes and ID is 1 byte, the storage space occupied by all CFs in node x is $5*(1+M)$ bytes; Because the number of sensor (N) in a BAN/BSN is less than 50 generally [1], and N nodes are deployed around a body of patient, therefore neighbors M is much smaller than N , so the space occupied by all CFs is relatively small.

6.2 Computational Overhead

There are two types of symmetric cryptographic primitives: stream ciphers and block ciphers. Stream ciphers typically operate on one bit of plaintext data to produce one ciphertext bit, while block ciphers may need to pad plaintext out to make the length of plaintext is a multiple of the block size; stream ciphers have low computation and energy overhead, but have not gained widespread confidence in their security strengths compared to block ciphers [28]. However, stream ciphers are still being widely used in wireless communications because of their fast operation and flexible implementation [28, 29]. In our protocol, we consider that Data2 is encrypted with a block cipher and Data1 with a stream cipher. Because the Data2 is encrypted only at the source node, the intermediate nodes do not need computation overhead and just forwards it; the Data1 is encrypted again after decryption for obtaining route information at the intermediate node, it needs some computation overhead, because of using a stream cipher and short Data1, the computation overhead is acceptable. If common XOR operation is considered in a stream cipher, the length of source and destination are 2 bytes (each needs 1 byte), the producing time length of data is 4 bytes, and CPU is 16 bits, encryption and decryption of Data1 at an intermediate node are required 3 XOR operations.

6.3 Energy Overhead

In the system initialization phase, the sink has broadcasted three messages (T_1 , T_2 and "OK"), node x $(1 \le x \le N)$ sends its CF once, receives M CFs of its neighbors, and may forwards CFs of other nodes (Non neighbors) many times, these are the extra energy cost in our protocol compared to other preloaded key schemes; but the amount of data is smaller and most of the battery of nodes can be replaced in the BAN/BSN, these energy consumptions are acceptable due to very few system initialization operations. In addition, when a source node sends a data packet to the sink, the intermediate node needs to encrypt Data1 again after decryption; the increased computation overhead will also consume certain energy, but the this energy consumption is negligible compared with energy consumption in sending and receiving data.

7. Conclusions

In this paper, we have presented a secure multi-hop data transmission protocol based on combination of node's clock characteristics and properties of the BAN/BSN. We exploit the dynamic and unique CFs of nodes, two kinds of pair-wise are generated under control of sink in a safe environment, one used to encrypt sensing data of a node and another used to encrypt routing information without relying on any pre-distributed secret information and added hardware, and a novel solution that establishes an secure routing of mutual authentication is described with improved AODV protocol. We analyze the security and performance of the presented protocol, it has good security in dynamic and accurate key, passive and active attacks, preventing node capture and supporting new node joining, and has accepted overheads of memory, computation and energy consumption; it satisfies the requirements of "plug and play" without the help of added node's hardware, makes the complicated data security and privacy in the BAN/BSN become operable easily and practicable strongly.

References

[1] H. Alemdar and C. Ersoy. "Wireless sensor networks for healthcare: A survey", Computer Networks, vol. 54, no. 15, **(2010),** pp. 2688-2710.
[2] P. Kumar and H.-J. Lee, "Security Issues in Health Applications Using Wireless Medical Sensor Networks: A Survey", Sensor, vol. 12, no. 1, **(2012),** pp. 55-91.
[3] M. Nabi, T. Basten, M. Geilen, M. Blagojevic and T. Hendriks, "A Robust Protocol Stack for Multi-hop Wireless Body Area Networks with Transmit Power Adaptation", In Proc. of the Fifth International Conference on Body Area Networks, Corfu Island , Greece, **(2010)** September.
[4] R. Vaid and V. Kumar, "Security Issues and Remedies in Wireless Sensor Networks- A Survey", International Journal of Computer Applications, vol. 79, no. 4, **(2013),** pp. 31-39.
[5] B. S. Jangra and V. Kumawat, "A Survey on Security Mechanisms and Attacks in Wireless Sensor Networks", International Journal of Engineering and Innovative Technology (IJEIT), vol. 2, no. 3, **(2012),** pp. 291-296.
[6] R. Rautray and I. Sarangi, "A Survey on Authentication Protocols for Wireless Sensor Network", International Journal of Engineering Science and Technology (IJEST), vol. 3, no. 5, **(2011),** pp. 4253-4256.
[7] G. H. Zhang, C. C. Y. Poon and Y. T. Zhang, "A Review on Body Area Networks Security for Healthcare", ISRN Communications and Networking, vol. 2011, Article ID 692592.
[8] L. Shi, M. Li, S. Yu and J. Yuan, "BANA: Body Area Network Authentication Exploiting Channel Characteristics", In Proc. of the fifth ACM conference on Security and Privacy in Wireless and Mobile Networks, Tucson, Arizona, USA, **(2012)** April.
[9] K. Venkatasubramanian and S. Gupta, "Physiological Value-based Efficient Usable security Solutions for Body Sensor Networks", ACM Transactions on Sensor Networks (TOSN), vol. 6, no. 4, **(2010),** pp. 1-36.
[10] G. Wu, L. Yao, B. Liu, K. Yao and J. Wang, "A Biometric Key Establishment Protocol for Body Area Networks", International Journal of Distributed Sensor Networks, vol. 2011, Article ID: 282986.
[11] Z. Zhang, H. Wang, A. V. Vasilakos and H. Fang, "ECG-Cryptography and Authentication in Body Area Networks", IEEE Transactions on Information Technology in Biomedicine, vol. 16, no. 6, **(2012),** pp. 1070-1078.
[12] A. Banerjee, S. Gupta and K. Venkatasubramanian, "PEES: Physiology-based End-to-End Security for mHealth", In Proc. of the 4th Conference on Wireless Health, Maltimore, MD, USA, **(2013)** November.
[13] M. Li, S. Yu, J. D. Guttman, W. Lou and K. Ren, "Secure Ad Hoc Trust Initialization and Key Management in Wireless Body Area Networks", ACM Transactions on Sensor Networks, vol. 9, no. 2, Article no. 18, (2013).
[14] S. T. Ali, V. Sivaraman and D. Ostry, "Secret Key Generation Rate Vs. Reconciliation Cost Using Wireless Channel Characteristics in Body Area Networks", In Proc. of the IEEE/IFIP 8th International Conference on Embedded and Ubiquitous Computing, Hong Kong, China, **(2010)** December.
[15] B. Latre, B. Braem, I. Moerman, C. Blondia and P. Demeester, "A Survey on Wireless Body Area Networks", Wireless Networks, vol. 17, no. 1, **(2011),** pp. 1-18.
[16] P. Reindl, K. Nygard and X. Du, "Defending Malicious Collision Attacks in Wireless Sensor Networks", In Proc. of the IEEE/IFIP 8th International Conference on Embedded and Ubiquitous Computing, Hong Kong, China, **(2010)** December.
[17] L. Shi, J. Yuan, S. Yu and M. Li, "ASK-BAN: Authenticated Secret Key Extraction Utilizing Channel Characteristics for Body Area Networks", In Proc. of Sixth ACM Conference on Security and Privacy in Wireless and Mobile Networks, Budapest, Hungary, **(2012)** April.

[18] S. T. Ali, D. Ostry and S. Jha, "Securing Data Provenance in Body Area Networks using Lightweight Wireless Link Fingerprints", In Proc. of the 3rd International Workshop on Trustworthy Embedded Devices, Berlin, Germany, **(2013)** November.
[19] F. Lanze, A. Panchenko, B. Braatz and A. Zinnen, "Clock Skew Based Remote Device Fingerprinting Demystified", In Proc. of the IEEE Global Communications Conference, Anaheim, CA, USA, **(2012)** December.
[20] Z. Yang, L. Cai and Y. Liu, "Environment-Aware Clock Skew Estimation and Synchronization for Wireless Sensor Networks", In Proc. of the 31st Annual IEEE International Conference on Computer Communications, Orlando, Florida, USA, **(2012)** May.
[21] D.-J. Huang, W.-C. Teng and C.-Y. Wang, "Clock Skew Based Node Identification in Wireless Sensor Networks", In Proc. of the IEEE Global Telecommunications Conference, New Orleans, LA, USA, **(2008)** November.
[22] M. B. Uddin and C. Castelluccia, "Toward Clock Skew Based Wireless Sensor Node Services", International Journal of Sensor Networks, vol. 9, no. 1, **(2011),** pp. 24-37.
[23] C. E. Perkins, E. M. Royer and S. Das. "Ad hoc on Demand Distance Vector Routing". RFC3561, **(2003)** July.
[24] D.-J. Huang and W.-C.Teng, "A Defense against Clock Skew Replication Attacks in Wireless Sensor Networks", Journal of Network and Computer Applications, vol. 39, **(2014),** pp. 26-37.
[25] V. Ayatollahitafti, S. Shariatmadari and M. A.Ngadi, "Evaluation of Ad-Hoc Routing Protocols on Body Area Networks". International Journal of Electronics Communication and Computer Engineering, vol. 4, no. 2, **(2013),** pp. 523-527.
[26] National Institute of Standards and Technology (NIST), "Advanced Encryption Standard (AES)," Federal Information Processing Standard (FIPS), vol. 197, **(2001)** November.
[27] H. Cheng, H. M. Heys and C. Wang, "PUFFIN: A Novel Compact Block Cipher Targeted to Embedded Digital Systems", in Proc. of Euromicro Conference on Digital System Design (DSD 2008), Parma, Italy, **(2008)** September.
[28] X. Zhang, H. M. Heys and C. Li , "Energy Efficiency of Symmetric Key Cryptographic Algorithms in Wireless Sensor Networks", In Proc. of the 25th Biennial Symposium on Communications, Kingston, ON, Canada, **(2010)** May.
[29] N. Fournel, M. Minier and S. Ubeda, "Survey and Benchmark of Stream Ciphers for Wireless Sensor Networks", in Proc. of the 1st IFIP TC6 /WG8.8 /WG11.2 International Conference on Information Security Theory and Practices: Smart Cards, Mobile and Ubiquitous Computing Systems, Heraklion, Crete, Greece, **(2007)** May.

Authors

Tan Jin, he received Ph.D degree from Huazhong University of Science and Technology, Wuhan, China. Now he is an associate professor. Research interests: Wireless Sensor Network and Communication, Multimedie Technology.

Wang Yijing, she received the B.S. Degree from China Jiliang University, Hangzhou, China. Currently she is a master student of China Jiliang University. Research interests: Wireless Sensor Network.