International Journal of Applied Engineering Research ISSN 0973-4562 Volume 12, Number 18 (2017) pp. 7990-7997

Obfuscation-based Delay-Aware Confidential Data Discovery and Dissemination Protocol in Wireless Body Area Networks

Prameela. S
Ph.D Research Scholar, Department of Computer Science,
Government Arts College (Autonomous), Race Course Road, Coimbatore, Tamilnadu, India.
Orcid Id: 0000-0001-9571-2990

Dr. P. Ponmuthuramalingam
Associate Professor, Department of Computer Science ,
Government Arts College (Autonomous), Race Course Road, Coimbatore , Tami nadu, India.
Orcid Id: 0000-0002-1689-0955

Abstract

Among different communication technologies, Wireless Body Area Network (WBAN) has the most significant for real-time monitoring and reporting of patient's physiological data economically. Once the network is constructed, the necessary process is discovering and disseminating the data into the network via wireless media for adjusting the configuration parameters of the body sensors based on the different data discovery and dissemination protocols. Such protocols are focussed on ensuring the reliability and security vulnerabilities, however physical layer security and end-to-end delay management are not considered for improving the performance of packet transmission. Hence in this article, Physical Layer (PHY) security is also taking into account with end-to-end delay management. In this approach, initially data discovery and dissemination protocol based on the multiple one-way key hash chains are applied for the instantaneous authentication. Moreover, the end-to-end delay-aware optimization is introduced based on the Multi-hop Topology Formation Game (MTFG) theory for ensuring the Physical Layer (PHY) security. The end-to-end delay based PHY secrecy is measured by optimizing the Secrecy Outage Probability (SOP). In addition, the multiple one-way hash chains are obfuscated for improving the temporal privacy. Finally, the simulation results show that the efficiency of the proposed protocol which improves the security of transmissions in practice**.**

Keywords: Wireless body area network, Data discovery and dissemination, Physical layer security, Multi-hop topology formation game theory, Secrecy outage probability, End-to-end delay.

INTRODUCTION

A Body Area Network (BAN) also known as Wireless Body Area Network (WBAN) is one of the types of wireless network of wearable computing devices. Such networks and its designs are differed from wireless sensor networks in different characteristics such as security, power efficiency, etc. WBAN is consisting of small sensor devices which are either embedded to the body or implanted under the skin. A BAN according to the IEEE is referred as a communication standard optimized for device of low power and functions around the human applications including medical, consumer electronics, etc. It refers that BAN utilizes the lowest power sensors and used in various human applications.

A typical BAN network consists of sensors, accelerometers, processor, transceiver and a battery. These are used for identifying the location of the monitored individual information and transmitting the essential sign and motion readings to the care takers. There are different challenges in BAN including security and privacy, interoperability, data consistency, cost, constrained deployment, etc. Over the past decades, many researchers proposed different data discovery and dissemination protocols such as Drip and DIP for ensuring the security. Most of the protocols involve cryptographic schemes which may have the highest computation and communication cost for WBAN. A lightweight and confidential data discovery and dissemination (D.He, et al.) [1] have been proposed based on the utilization of multiple one-way key hash chains and also the unique features and application requirements of WBAN. This approach maintains the confidentiality and reduces the computational, energy and communication cost while securing the multi-hop dissemination of data. However, the delay-aware optimization of the physical layer security has not been considered which improves the further security of the network.

Hence in this article, delay-aware optimization of physical layer is proposed with data discovery and dissemination protocol for ensuring the security in multi-hop WBAN. The major contribution of this article is as follows:

- First, data discovery and dissemination protocol based on the multiple one-way key hash chains is investigated.
- Second, delay-aware optimization is introduced by using Multi-hop Topology Formation Game (MTFG) theory for enhancing the physical layer security. The average end-to-end delay for each sensor node is measured by using the different parameters such as traffic distribution, transmission time distribution, and service time distribution. The security cost and QoS measure of the each node is optimized based on the proposed protocol.
- In addition, the temporal privacy of the packet transmission is achieved by obfuscating the multiple one-way hash chains effectively.

The rest of the article is organized as follows: Section 2 presents the protocols which are related to ensure the physical layer security in WBAN. Section 3 explains the proposed protocol in multi-hop WBAN. Section 4 illustrates the performance evaluation of the proposed protocol. Section 5 presents the conclusion and future enhancement of the research work.

LITERATURE SURVEY

Interference mitigation was presented (Z. Zhang, et al.) [2] for physical wireless body area network using social networks. In this approach, inter-WBAN interference was modeled and distance between the distributions of the interference was computed based on both theoretical and practical analysis. Social interaction detection and prediction algorithms were developed for WBAN. The power control game was also developed based on social interaction information for maximizing the system's utility as minimize the energy consumption of WBAN system. However, the effectiveness of the method incorporated with MAC layer protocol was less.

The physical layer security was investigated (A. Mukherjee, et al.) [3] in multi-user wireless networks. Initially, broad review about the physical layer security was provided in multi-user wireless networks. The evaluation of the protected transmission approaches from point-to-point channels to multiple antenna systems and multi-user broadcast, multiple access interference and relay networks were described. Secret key generation and physical layer mechanisms according to the protocols were also explained. Subsequently, secrecy based on channel coding methods was examined including with the game theory and stochastic geometry approaches. The physical layer message authentication was also briefly explained.

Fuzzy attribute based signcryption scheme was proposed (C.Hu, et al.) [4] for body area network security. A novel security mechanism called Fuzzy Attribute-Based Signcryption (FABSC) was introduced for providing the proper trade-off between security and elasticity. This mechanism was based on the combination of digital signatures and encryption process to provide confidentiality, authenticity, un forge ability and collusion resistance. Also, the effectiveness of this mechanism was proved by theoretically. However, the computation and storage cost of this method were high.

A protocol was proposed (A.S. Kumar, et al.) [5] for the secure distributed data discovery and dissemination in wireless sensor networks. This method was mostly used to update the configuration parameters and to distribute the management instructions in wireless sensor networks. This system establishes the novel protocol called DiDrip for protected and distributed data discovery and dissemination. However, messages can easily interrupt since open nature of wireless channels.

A protocol (R. Nath, & P.K.Sehgal,)[6] was proposed for secure and dynamic data dissemination in mobile Ad Hoc network. In this scheme, the security issues in data discovery and dissemination protocols for WBAN were identified. This approach uses extend of Drip protocol based on the use of multiple one-way key hash chains. Also, extension of Adhoc On-demand Distance Vector (SD-AODV) routing protocol was proposed to achieve high efficiency. However, this protocol was computationally inefficient.

ECG-cryptography and authentication were proposed (Z.Zhang, et al.) [7] in body area networks. Initially, a novel biometric-based approach was developed for authenticating the message based on the lightweight fashion in body area networks. Then, a novel key agreement technique was proposed which allows the neighbouring nodes in body area networks for distributing the common key generated by electrocardiogram (ECG) signals. In addition, an Improved Jules Sudan (IJS) algorithm was proposed for setting key agreement used for the message authentication. However, the performance of the approach requires further improvement by including additional unique features.

Lightweight security and authentication were proposed (A.S.Sangari, & J.M.L. Manickam,) [8] in wireless body area network. In this approach, a low cost and high quality electro cardiograph and diagnostic system were proposed for healthcare applications. The algorithm was proposed for avoiding the main problem such as preserving the security and privacy of patient's medical healthcare information over wireless communications. The secret key encryption algorithm named Skipjack was proposed for providing the secure communication between sensor node and mobile node. However, this approach was not used for large-scale networking system.

PROPOSED METHODOLOGY

In this section, the proposed delay-aware optimization with data discovery and dissemination is briefly explained. This approach is used for avoiding the delay which degrades the security due to the loss of packets in WBAN.

Assumptions

The following assumptions are considered for the proposed protocol

- Assume the base station is non-compromised and trustworthy for source of dissemination since it is untrustworthy.
- The considered body sensors are resource constrained in terms of storage, power consumption, bandwidth and energy. Since constrained resources are computationally costly and energy intensive functions are not achieved for these nodes.

Network Model

Consider the WBAN which consists of N number of body sensor nodes that are transmits their sensed data to the common hub H in the uplink and W is denoted as passive wire tappers that are presented in the vicinity and can individually tap into the sensor node's communications. Consider that statistical Channel State Information (CSI) for both legitimate and wiretap channels is available at the transmitter such that the mean and standard deviation of the received Signal-to-Noise Ratio (SNR) is estimated for each transmitter node. The packets are transmitted by the base station and received by each body sensor node through one or two hops. Since, this two-tier architecture is mostly crucial for improving the network capacity and scalability, reducing the system complexity, prolonging the network lifetime and ensuring the highest level of security and privacy by reducing the end-to-end delay.

Threat Model

Consider the adversary is computationally resourceful entities like desktop PC. The threats are launched by either internal or external attacks. In external attacks, all the traffic is interfered, arbitrary messages are inserted, old messages are replayed, node identities are spoofed and the communication channel is blocked by an impostor. In addition, Denial-of-Service (DoS) attacks are launched by an adversary in order to consume the limited resources on the selected nodes. In internal attacks, the number of nodes is physically compromised by an adversary and the cryptographic keys are extracted from them for launching the attacks on the network.

Initialization Phase

The proposed protocol has multiple one-way hash chains based on the function $H(\cdot)$. By applying $H(\cdot)$ to an initial element frequently for b times, the hash chain with length b is generated. The last value after $H(\cdot)$ has been applied b times is called as the committed value of the hash chain. Initially, the nodes are separated into K groups based on their hop distance from the base station. The hash chains are constructed before the deployment of nodes. The $(b-i)^{th}$ output of hash function is denoted as $K_{i,j}$ which is derived from j^{th} random seed number $K_{b,j}$. The length b of each chain is arbitrary but no less than the number of data items that the base station requires for disseminating in the network lifetime.

The representation of data item used in the proposed protocol is {*order*, *key*, *version*, *data*} where, $order$ is the dissemination orders of the data item, key is used for identifying uniquely the concerned variable, *version* is used for indicating whether the data item is new or not and *data* is the disseminated value for the concerned variable.

Packet Pre-processing and Verification Phase

Once network is initialized, the base station generates the packet through concatenating the data item d and the successor keys for disseminating the data item $d = \{order, key, version, data\}$ by the base station. Then, the data item is encrypted with the symmetric encryption method by using the successor keys. The pre-processing (PP_i) for i^{th} data item $(d_i = \{order_i, key_i, version_i, data_i\})$ which is propagated to N hops is expressed as follows:

$$PP_i = E(\{d_i, K_{i-1}\}, K_{i-1,1}) \| \cdots \| E(\{d_i, K_{i,N}\}, K_{i-1,N}) \quad (1)$$

In equation (1), $order_i = 1$ and $1 \le i \le b$. The target nodes identity information is added in the packet header which means the destination field of the packet. For this situation, each cryptographic hash $H(\cdot)$ measured over the destination field which ensures its authority and integrity.

Based on the received packet $(PP_i)$from one hop neighboring node or the base station, each sensor node S_k retrieves the correct group information from (PP_i) that refers the node parses the right field $E(\{d_i, K_{i-1}\}, K_{i-1,1})$ and then uses the key $K_{i-1,1}$ for performing $D(E(\{d_i, K_{i-1}\}, K_{i-1,1}), K_{i-1,1}) = \{d_i, K_{i,1}\}$

for decrypting the cipher text. After that, the following functions are performed by the node S_k

- If this is a new data item, then the node verifies whether the received key $K_{i,1}$ hashes to the stored $K_{i-1,1}$. If the outcome is positive, then the

authenticity and integrity of the packet is assured and the packet is accepted or else the packet is discarded.

- If the node has an identical data packet, then it increases the broadcast interval of the packet through the Trickle algorithm which limits the energy costs while the network is consistent.
- If this is an old data packet, then the node broadcasts its stored data packet.

This protocol ensures the dynamic data, data confidentiality, delay tolerance, and immediate authentication. However, the PHY security problem due to high delay is not considered which also degrades the network security performance by discarding the more number of packets. Hence, the end-to-end delay is measured in terms of traffic distribution, transmission time distribution, and service time distribution (H. Moosavi, &F.M. Bui) [9].

End-to-End Delay Measurement

Traffic Distribution

The traffic load of each sensor node is unique. Therefore, the packet service time at each node is also differed from each other nodes since it depends on the characteristics of the medium access protocol and the physical constraints. Consider each sensor node acts as a one server which has the ability for handling the one packet at a time with a service discipline of First-Come First-Served (FCFS).

The traffic load of each sensor node is measured based on the network topology and inter-arrival distributions of the packets. Consider the inter-arrival distribution of packets at the MAC layer of node (n) by A_n with moment generating function (M_{A_n}) and the inter-arrival time of packets received successfully from the children node which is relayed in the uplink with the moment generating function $(M_{A_n}^{C_n})$ are statistically independent to each other. The overall moment generating function is given as follows

$$M_{A_n}(t) = M_{A_n}^{n}(t) M_{A_n}^{C_n}(t) \qquad (2)$$

In equation (1), C_n is the set of children of a node $(n \in N)$. The inter-arrival distribution of packets received successfully by the node is referred the combined inter-departure times of packets from the children nodes. Therefore, $M_{A_n}^{C_n}$ is computed based on the inter-departure distribution of packets from children node with the moment generating function M_{D_c} and is given below

$$M_{A_n}^{C_n} = \prod_{c \in C_n} M_{D_c}(t) \qquad (3)$$

The moment generating function of the inter-departure distribution of packets from the node is computed based on the moment generating functions of the inter-arrival time and the service time of packets (S_n) at node n.

$$M_{D_n}(t) = \gamma_n M_{S_n}(t) + (1-\gamma_n) M_{S_n}(t) M_{A_n}(t) \qquad (4)$$

In equation (4), $\gamma_n = \frac{\varepsilon[S_n]}{\varepsilon[A_n]}$ denotes the utilization factor of the node n. For preventing an over-saturated condition in the network, consider $\gamma_n \leq 1 \; \forall n \in N$ and also the transmission rate of each node is greater than the accumulated traffic rate forwarded by the node. Hence, the expected and variance values of the packet inter-arrival time at each sensor node are obtained.

Transmission Time Distribution

Each sensor node in the considered WBAN shares the wireless medium by using the slotted Aloha. Each Aloha slot is greater than or equal to the time required for packet transmission which is given as,

$$\tau = \frac{L_b}{R_d} + \varepsilon \approx \frac{L_b}{R_d} \qquad (5)$$

In equation (5), L_b is the packet length in bits, R_d is the rate of data transmission, and ε is the time taken by the node for receiving an ACK/NACK from its destination and it is negligible. The probability distribution for the time required for packet transmission from the instance node n initiates the slotted Aloha access process until it completes the transmission is denoted as T_n and its geometric distribution with the probability mass function is given as follows:

$$Pr\{T_n = k\tau\} = CP_n(1-CP_n)^{k-1}, k = 1,2,\ldots \qquad (6)$$

In equation (6), CP_n refers the contention probability which is maintained by the node n. After that, the moment generating function of the transmission time distribution from the node n is given by,

$$M_{T_n}(t) = E[e^{tT_n}] = \sum_{k=1}^{\infty} \Pr\{k\tau\} \cdot e^{tk\tau} = \frac{CP_n \cdot e^{tk\tau}}{1-(1-CP_n)\cdot e^{tk\tau}} \qquad (7)$$

Service Time Distribution

The service time distribution is measured based on the probability of a successful packet transmission which is

depends on whether a collision occurs or not and the received SNR. The average probability of successful packet transmission for node n is given as,

$$\delta_n = 1 - [\chi_n + (1 - \chi_n)\zeta_n] \quad (8)$$

$$\chi_n = 1 - \prod_{x \in N \setminus \{n\}} (1 - \gamma_x) \quad (9)$$

$$\zeta_n = 1 - \left[1 - \frac{1}{2} exp(-\bar{\alpha}_n)\right]^{L_b} \quad (10)$$

In above equations, χ_n is the collision rate of a packet transmitted by the sensor node and ζ_n is the packet error rate of node n while no collision occurs also known as a function of the received SNR from transmitter n. Then, the moment generating function of the probability distribution of service time at node n is given as follows:

$$M_{S_n}(t) = \sum_{k=1}^{\infty} \delta_n (1 - \delta_n)^{k-1} M_{T_n}^k(t) \quad (11)$$

Therefore, the average and variance of the service time at node n are obtained by using the equations (7) & (11) respectively.

$$E[S_n] = M'_{S_n}(t)|_{t=0} = \frac{8}{3}\tau \left(\frac{2}{\delta_n} - 3\delta_n + 2\delta_n^2\right) \quad (12)$$

$$V[S_n] = M''_{S_n}(t)|_{t=0} - E[S_n]^2 = \frac{\tau^2}{9}\left(\frac{256}{\delta_n^2} - \frac{48}{\delta_n} + 768 - 1976\delta_n + 528\delta_n^2 + 768\delta_n^3 - 256\delta_n^4\right) \quad (13)$$

End-to-End Delay

The moment generating function of the total packet delay at the node n is approximately computed by using the moment generating functions of inter-arrival time and service time of packets at a node n. (Baz, M., et al. 2015)

$$M_{\Delta_n}(t) = \frac{(1 - E[A_n]E[S_n])(t-1)M_{S_n}(t)\left(1 - M_{A_n}\left(M_{S_n}(t)\right)\right)}{E[A_n]\left(1 - M_{S_n}(t)\right)\left(t - M_{A_n}\left(M_{S_n}(t)\right)\right)} \quad (14)$$

By using the equation (14), the average packet delay at node n is computed as follows:

$$E[\Delta_n] = E[S_n] + \frac{E[S_n]V[A_n] + E[A_n]V[S_n]}{2(1 - E[S_n]E[A_n])} \quad (15)$$

The average end-to-end delay by a packet over the K-hop transmission path $l_n = \langle m_1, \ldots, m_{K+1} \rangle$ is the collection of the delays at the nodes and is given as follows:

$$E[\Delta'] = \sum_{k=1}^{K} E\left[\Delta_{m_k}\right] \quad (16)$$

Thus, the end-to-end delay of the packet transmission at each node is calculated which is further utilized for measuring the security cost and QoS measure based on the Multi-hop Topology Formation Game (MTFG) theory for identifying the secrecy level of transmission through WBAN.

Formulation of Security Cost and QoS Measure

Initially, consider the MTFG denoted by $G = \langle N, \{S_n\}, \{c_n\} \rangle$ where N refers the set of players with the element n, S_n refers the set of strategies of player n with the strategy s_n corresponding to the selection of the next-hop node in the uplink, and c_n refers the cost function associated with the player n. Consider the network graph $G(V, E)$ in which the sensor node $n \in N$ selects for connecting to the node s_n from its strategy space in the uplink and forms a K-hop transmission path to the hub.

The security cost function of node n is formulated as the Secrecy Outage Probability (SOP) of its transmission path to the hub.

$$c_n(G) = P_{l_n}^{out} = 1 - \prod_{k=1}^{K}\left(1 - P_{\langle m_k, m_{K+1}\rangle}^{out}\right)$$

$$= P_{\langle n, s_n\rangle}^{out} - \left(P_{\langle n, s_n\rangle}^{out} - 1\right)\left[1 - \prod_{k=2}^{K}\left(1 - P_{\langle m_k, m_{K+1}\rangle}^{out}\right)\right]$$

$$= P_{\langle n, s_n\rangle}^{out} - \left(P_{\langle n, s_n\rangle}^{out} - 1\right)c_{s_n}(G) \quad (17)$$

The above security cost function is used for identifying the transmission performance in terms of PHY security. Furthermore, the QoS measure of the node n is also formulated as the average end-to-end packet delay.

$$q_n(G) = E[\Delta^{l_n}] = \sum_{k=1}^{K} E\left[\Delta_{m_k}\right] = E[\Delta_n] + \sum_{k=2}^{K} E\left[\Delta_{m_k}\right]$$

$$= E[\Delta_n] + q_{s_n}(G) \quad (18)$$

The average end-to-end packet delay should be less than or equal to an upper bound (ρ_n) for each sensor node n. This delay constraint facilitates the hub or sensor nodes for specifying the maximum tolerable end-to-end delay in the WBAN for scheduling the uplink or downlink allocation interval periods or real-time monitoring requirements. Thus, the PHY security is improved by reducing the computational cost and end-to-end packet delay over the transmission path. In addition, the obfuscation of the multiple one-way hash chains is exploited for achieving the temporal privacy. Obfuscation is an algorithm used for security applications. The obfuscation is done based on their parameter values which are infrequently available to the adversary. They are randomly selected from the definite set of numbers which map to a single value. The set of possible values for a variable should be large enough and be randomly distributed.

EXPERIMENTAL RESULTS

In this section, an effectiveness of the proposed protocol is evaluated by implementing its components in an experimental test-bed. The analysis is based on the different metrics such as end-to-end delay, energy consumption, packet delivery ratio, throughput, and coverage time. The simulation parameters are given in Table 1.

Table 1: Simulation Parameters

Parameters	Values
Number of body sensor nodes	54
Channel type	Wireless channel
Propagation model	Two Ray Ground
MAC layer	IEEE 802.11
IFQ type	Queue/DropTail/PriQueue
Link layer	LL (Link Layer)
Physical type	WirelessPhy
Antenna type	Omni Antennas
IFQ length	1000
Routing protocol	AODV

End-to-End Delay

End-to-end delay refers the time period taken for the data packets to be transmitted from source node to destination node over the communication channel. It is measured based on the different parameters like traffic, transmission time, and service time. It is computed by using the following formula

End-to-end delay=

$$\frac{\text{Total delay of packets received by the destination}}{\text{Number of packets received by the destination}}$$

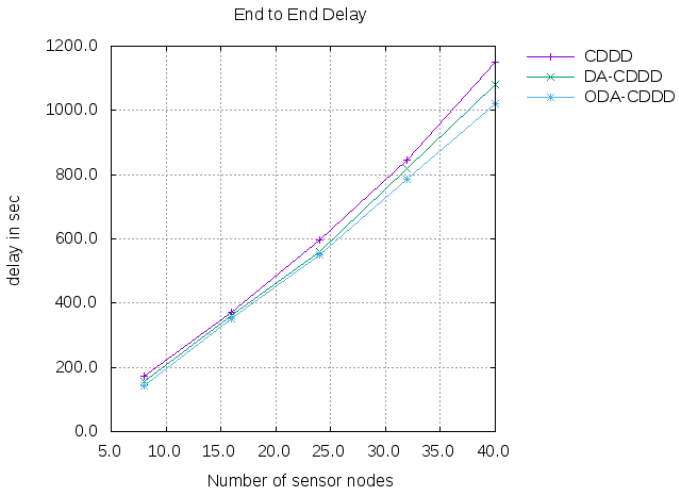

Figure 1: End-to-end Delay

Figure 1 shows that the comparison of end-to-end delay made between Confidential Data Discovery and Dissemination (CDDD), Delay-Aware CDDD (DA-CDDD) and the proposed Obfuscation Delay-Aware CDDD (ODA-CDDD) protocols. In the graph, number of sensor nodes is taken in x-axis and delay values are taken in y-axis which is measured in seconds. It proves that the ODA-CDDD protocol has less end-to-end delay compared with the other protocols.

Energy Consumption

Energy consumption is defined as the amount of energy consumed by the network for transmitting the data packets to the destination within the given delay.

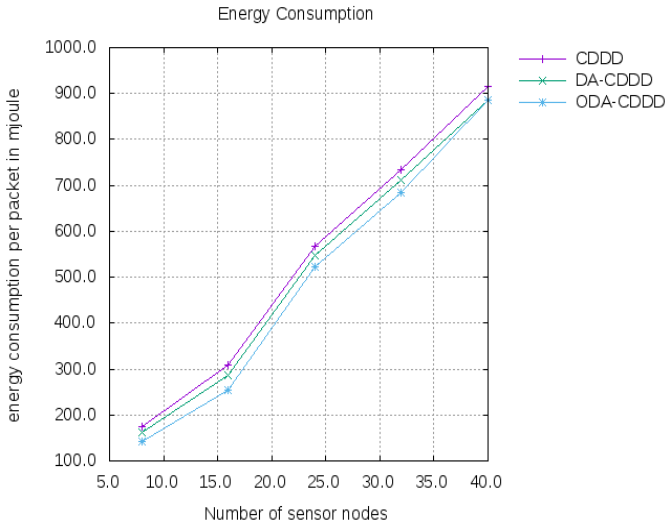

Figure 2: Energy Consumption per Packet

Figure 2 shows that the comparison of energy consumption made between CDDD, DA-CDDD and ODA-CDDD

protocols. In the graph, number of sensor nodes is taken in x-axis and energy consumption per packets is taken in y-axis which is measured in milli Joules. It proves that the ODA-CDDD protocol has less energy consumption compared with the other protocols.

Packet Delivery Ratio

Packet Delivery Ratio (PDR) refers the fraction between total number of data packets received and total number of data packets transmitted over the communication medium. It is measured by the formula given as,

$$PDR = \frac{Number\ of\ data\ packets\ received}{Number\ of\ data\ packets\ transmitted}$$

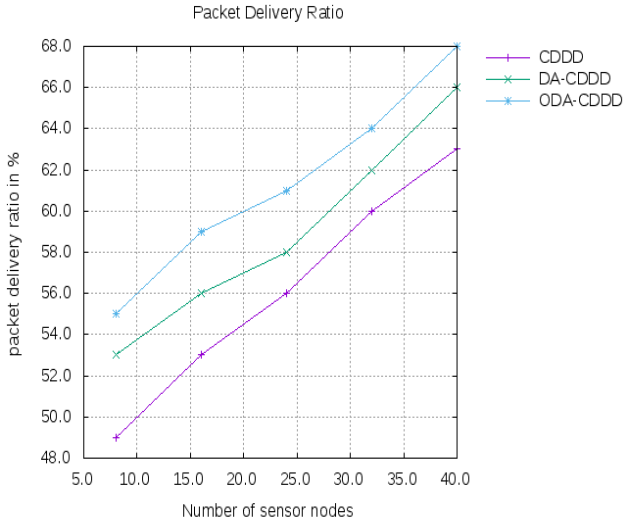

Figure 3: Packet Delivery Ratio

Figure 3 shows that the comparison of packet delivery ratio made between CDDD, DA-CDDD and ODA-CDDD protocols. In the graph, number of sensor nodes is taken in x-axis and PDR (%) is taken in y-axis. It proves that the ODA-CDDD protocol has better PDR compared with the other protocols

Throughput

Throughput is defined as the number of data packets forwarded to the destination within the given time period and its unit is bits per second (bits/sec). It is calculated by using the following formula

$$Throughput = \frac{Total\ number\ of\ forwarded\ data\ packets}{Time\ duration}$$

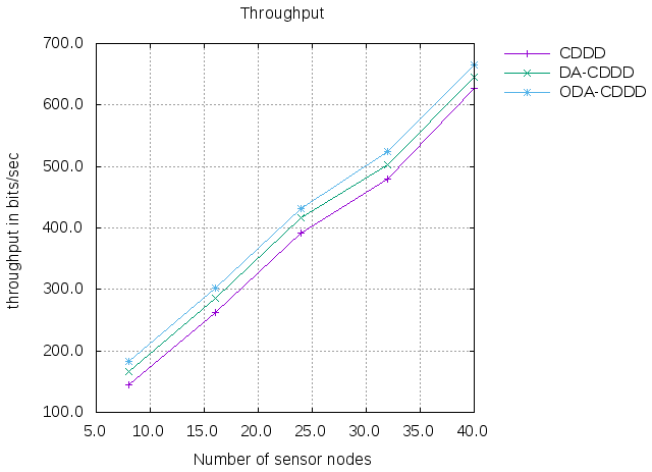

Figure 4: Throughput

Figure 4 shows that the comparison of throughput made between CDDD, DA-CDDD and ODA-CDDD protocols. In the graph, number of sensor nodes is taken in x-axis and throughput is taken in y-axis which is measured in bits/seconds. It proves that the ODA-CDDD protocol has better throughput compared with the other protocols.

Coverage Time

Coverage time is defined as the time duration for successfully achieving the packet transmission with high level of security over the communication channel.

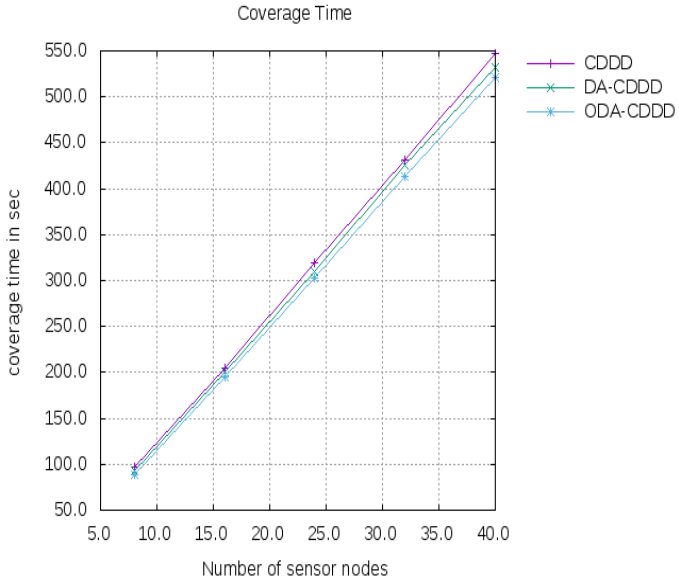

Figure 5: Coverage Time

Figure 5 shows that the comparison of coverage time made between CDDD, DA-CDDD and ODA-CDDD protocols. In

the graph, number of sensor nodes is taken in x-axis and coverage time is taken in y-axis which is measured in seconds. It proves that the ODA-CDDD protocol has less coverage time compared with the other protocols.

CONCLUSION

In this article, data discovery and data dissemination protocol by using the multiple one-way key hash chains is studied and addressed the PHY security vulnerabilities and end-to-end delay issues in data discovery and dissemination of WBAN. Therefore, end-to-end delay management is considered with the PHY security based on the optimization approach. A Multi-hop Topology Formation Game (MTFG) theory is proposed for formulating the end-to-end delay and PHY security. This approach maintains the minimum SOP and end-to-end delay requirements in WBAN. Moreover, the temporal privacy of the packet transmission is exploited based on the obfuscation of multiple one-way key hash chains. The experimental analysis proves that the Obfuscation-based Delay-Aware Confidential Data Discovery and Dissemination protocol improves secrecy level and reduces the delay constraints.

REFERENCES

[1] D. He, S. Chan, Y .Zhang, and Yang. "Lightweight and confidential data discovery and dissemination for wireless body area networks". IEEE journal of biomedical and health informatics, 18(2), pp. 440-448, 2014.

[2] Z. Zhang, H. Wang, C. Wang, and H. Fang. " Interference mitigation for cyber-physical wireless body area network system using social networks". IEEE transactions on emerging topics in computing, 1(1), pp. 121-132,,2013.

[3] A. Mukherjee, S.A.A. Fakoorian , J.Huang, and A.L. Swindlehurst. " Principles of physical layer security in multiuser wireless networks: A survey" . IEEE Communications Surveys & Tutorials, 16(3), pp. 1550-1573, 2014.

[4] C. Hu, N. Zhang, H. Li, X. Cheng and X. Liao. "Body area network security: a fuzzy attribute-based signcryption scheme". IEEE journal on selected areas in communications, 31(9), pp. 37-46 ,2013.

[5] A.S.Kumar, S. Velmurugan and E. Logashanmugam "A secure distributed data discovery and dissemination in wireless sensor networks".International Journal of Engineering & Science Research, 5(7), pp. 708-713,2015.

[6] R.Nath. and P.K. Sehgal. " SD-AODV: A Protocol for Secure and Dynamic Data Dissemination in Mobile Ad Hoc Network". arXiv preprint arXiv:1107.3363,2011.

[7] 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, 16(6), pp. 1070-1078, 2012.

[8] A.S. Sangari and J.M.L Manickam. "Light weight security and authentication in wireless body area network". Indian Journal of Computer Science and Engineering, 4(6), pp. 438-446,2013.

[9] H. Moosavi and F.M. Bui. "Delay-aware optimization of physical layer security in multi-hop wireless body area networks ". IEEE Transactions on Information Forensics and Security, *11*(9), pp. 1928-1939, 2016.

[10] M.Baz ,P.D.Mitchell, and D.A. Pearce. "Analysis of queuing delay and medium access distribution over wireless multi hop pans", IEEE Transactions on Vehicular Technology, 64(7), pp. 2972-2990,2015.