Advanced Threat Defense with Load Equilibrium Cluster Head Selection in WSN

[1]Reshma G, [2]Jeejo K P
[1]P G Scholar, [2]Assistant Professor
[1]Department of Electronics and Communication Engineering,
[1]A P J Abdul Kalam Technological University,
[1]Thejus Engineering College, Kerala, India

Abstract : Wireless Sensor Networks (WSN) helps in information gathering and are effectively employed in several applications nowadays. Energy is a meagre resource for these sensor networks as sensor nodes are powered by battery sources. Also sensor networks may deal with crucial information that must be safeguarded from attackers. Thus energy efficiency and information security have got paramount importance while designing an efficient WSN. Thus after analyzing the earlier methods, to avoid those issues a new prototype called 'Advanced Threat Defense with Load Equilibrium CH Selection in WSN' is created. To reduce the energy consumption of the network balanced load clustering is done and the security to the data packets is provided using elliptic curve method. Simulation results show how this approach performs better than earlier methods in terms of energy efficiency, packet delivery ratio, packets drop and network delay.

IndexTerms **- WSN, energy efficiency, clustering, security, ECC.**

I. Introduction

Nowadays smart environments find applications in several areas. Military, environment, industry, agriculture, health care, intelligent transportation, infrastructure monitoring, threat detection are few among them. Smart environments usually rely on Wireless Sensor Networks (WSN) for data collection and data communication. WSN are infrastructure less and self-configurable network that allows easy to use and flexible installations and this enables them to be used in a wide variety of applications. WSN is a sensor network which consists of large number of low power and low cost sensing devices, called nodes, that have limited energy, memory and processing capabilities. These nodes are capable of monitoring physical or environmental conditions like pressure, temperature, sound, humidity, wind etc. After data acquisition they process the data and transmit it to the destination.

Nevertheless, there are several challenges for WSN due to its constraints. Due to the limited battery source there is a need to optimize their energy resources because once its energy gets depleted it will be impractical to replace or recharge them as they are deployed in unattended harsh environments. And the failure of one node may cause the disruption of the entire system or application. Also in addition to this security is also a major concern since WSN work with sensitive data which is susceptible to threats of diverse nature like Black hole attack, Sybil, Wormhole, Flooding and so on. To ensure that the data being received and transmitted across these networks is secure and protected, information security plays a vital role. So there is a need to design an energy efficient and secure system which works impeccable with the resource constrained sensor networks.

Cluster based Energy Efficient Trust Management mechanism (CEETM) is an energy efficient trust management model based on three tier architecture. This system could provide energy efficiency and security to medical wireless sensor Network but at the same time suffers from low QoS parameters.

Thus after analyzing the earlier methods, to avoid those issues we have created the new prototype called as Advanced Threat Defense with Load Equilibrium CH Selection in WSN. To reduce the energy consumption clustering scheme which incorporates balanced load concept is used in this network and the idea of hybrid MAC (h-MAC) provides two channels (TDMA & CSMA) for data transmission during increase in traffic load or during an emergency packet transmission thus helps in interference management. It helps to improve energy efficiency without affecting throughput [1].Since wireless sensor nodes have limited computing power, data storage and communication capabilities, any security protocol must be designed to operate efficiently in a resource constrained environment. So Elliptic Curve Cryptography (ECC) is the best candidate. ECC got attention due to its smaller key size. With smaller keys it can provide the same level of security as provided by larger keys of other public key cryptographic systems. It is mostly useful for resource constrained applications as it has the capability to provide high level security with low computing power and battery resource. The other advantages of smaller key sizes include speed, efficient use of power & bandwidth, lower space requirements for key storage & quicker arithmetic operations [2]. So Security to the data packets is provided using Elliptic Curve Method. Two major attacks affecting WSN are considered for implementation. They are Black hole attack and Sybil attack. Interference management is achieved through hybrid Medium Access Control (h-MAC) mechanism. And finally during the performance analysis the results like energy efficiency, energy consumption, packet delivery ratio, packet drop and network delay is calculated and compared with existing systems.

The rest of the paper is organized as follows. Section II presents the related work. Section III explains the proposed model. Section IV presents the simulation results and the paper is concluded in Section V.

II. RELATED WORK

A brief introduction of the WSN, energy conservation, node deployment, its applications, main features, and key technologies is given in [3]. To increase the network lifetime energy efficiency becomes the biggest requirement in sensor network [4]. It has been concluded that of all transmission techniques, gateway communication and clustering are considered as the best approaches for data transmission and it gives better performance in terms of energy efficiency and longer lifespan. Several protocols are proposed to enhance the life time of WSN, of them the clustering based hierarchical protocols are popular due to their high energy efficiency. Energy efficient protocol was proposed by Heinzelman in [5] called Low-Energy Adaptive Clustering Hierarchy (LEACH). However LEACH protocol has got certain drawbacks. To overcome the shortcomings of LEACH and to make it more efficient many descendants of LEACH protocol are introduced like LEACH-E, LEACH-EEE, LEACH-K, LEACH M, LEACH-MR, LEACH-TL, DD LEACH [6].

A new wireless MAC mechanism that modifies IEEE 802.15.4 standard to provide energy efficient, reliable and delay bounded data transmission for hybrid monitoring applications is presented in [7]. The design and implementation of h-MAC on IEEE 802.11 standard to overcome performance degradation due to co-channel interference is presented in [8]. CSMA/CA & TDMA hybrid scheme protocol (CTh-MAC) is proposed for mobile WSN to improve the energy efficiency [9].

The basics of information security with special emphasis on WSNs, some of the major attacks on WSN along with their preventive and counter steps is provided in [10,11]. Several WSN user authentication protocols and their drawbacks are reviewed in [12]. The paper concludes that ECC-based protocol is shown to be suitable for higher security WSNs. Authors in [13] discusses different issues of WSN and the relevance of ECC. The paper concludes that ECC is an excellent choice for asymmetric cryptography in power constrained devices. The advantages include smaller key sizes, speed, efficient use of power and bandwidth, lower space requirements for key storage and quicker arithmetic operations.

III. PROPOSED SYSTEM

This paper proposes an improvised architecture for WSN by incorporating clustering scheme with Elliptic curve method to provide energy efficient and data authenticated system.

Sensor nodes are grouped into clusters where each cluster will be headed by a Sub -Cluster Head (SCH). Child node will hand on the information to the sub cluster head. The Cluster Head (CH) and the Base Station (BS) are located so far from the field where the nodes are localized. So a SCH cannot directly transfer the data to the CH due to high energy depletion. So to address this issue Mobile sink Node (MN) is introduced. The mobile sink node will act as an intermediate between the SCH and the CH. It moves from one place to another and gather the information from nearby sub cluster heads and transmits it to the CH.CH then performs data aggregation and transmit it to the Base Station (BS).

Usual data transfer between nodes makes use of TDMA methodology. But when there is an increase in traffic load or emergency packet transmission occurs then high priority region based data transmission is initiated. If any node is identified that in this region, those neighbour nodes holds the data and shifted over to CSMA and provides the current slot to the node which is in the high priority region. At the end TDMA mode will be activated.

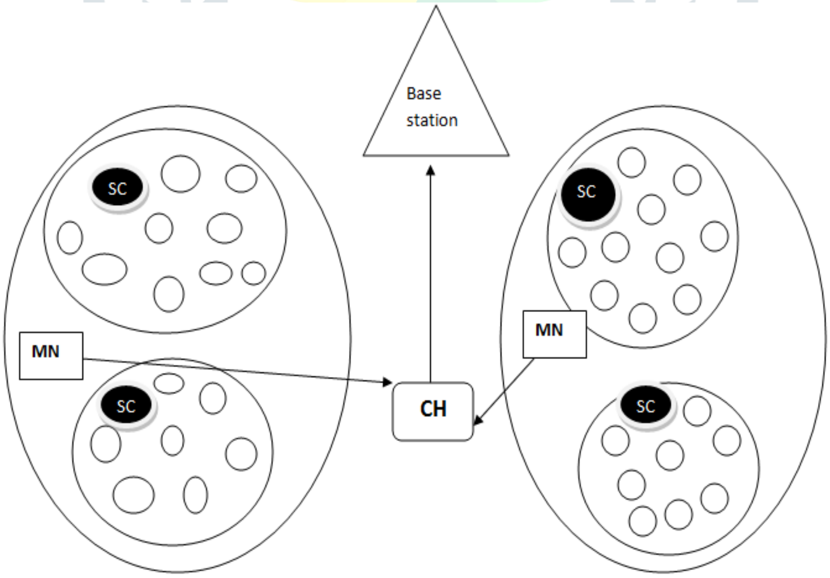
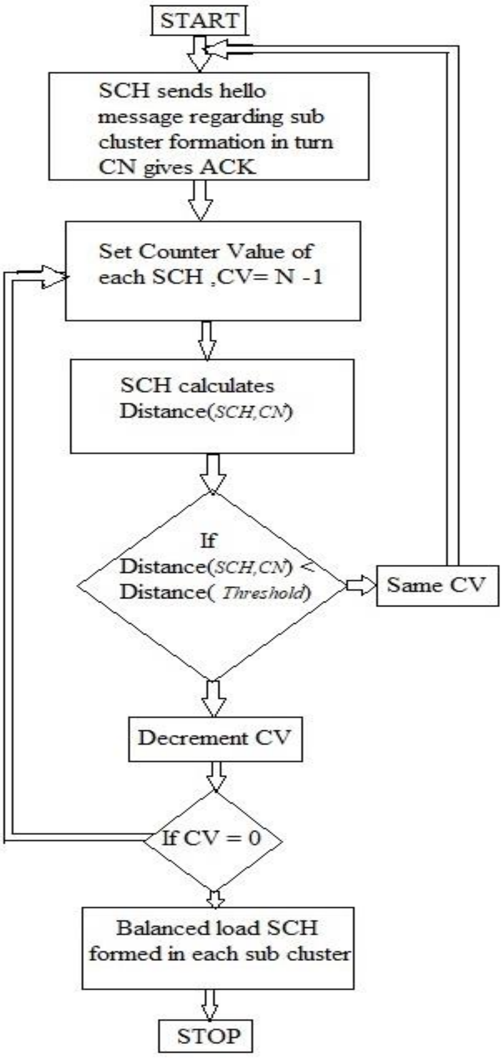


Fig 1: Architecture of proposed system

To reduce the energy consumption and thus to increase the network life time load must be balanced with in a network. If few sub-cluster nodes are heavily loaded, it will lead to faster energy consumption and can cause node failure which may affect the overall network. So to get normal depletion of energy the balanced load sub cluster head selection is initiated. The distance between the normal child nodes and the sub cluster head plays a major part in energy consumption. So, balanced load sub cluster head selection leads to nominal energy depletion of each node is present in the network by making transmission with closer nodes only.

Algorithm for Balanced Load Sub-cluster head selection:


START
SCH sends hello message regarding sub cluster formation in turn CN gives ACK
Set Counter Value of each SCH ,CV= N -1
SCH calculates Distance(SCH,CN)
If Distance(SCH,CN) < Distance(Threshold)
Same CV
Decrement CV
If CV = 0
Balanced load SCH formed in each sub cluster
STOP

Initially, the SCH nodes will send hello packets to all the nearby nodes and the nodes will send back the acknowledgement. TDMA MAC scheduling technique is introduced here to avoid collision. According to the receipt of an acknowledgment all SCH nodes compare the distance between itself to the child nodes with the threshold distance. After calculating the distance, each SCH nodes will sends the message to the concerned child nodes which are near to it. Thus a balanced load SCH will be formed in each cluster. If the child receives more than one number of copies then it will randomly select the SCH node which it has to coordinate.

$$\text{Distance}_{(\text{SCH})(\text{CN})} = \sqrt{\text{SCHi}(x,y) - \text{CNj}(x,y)}$$

where i = 1,2,3,…… are SCH nodes and j = 1,2,3, … are child nodes.

Elliptic Curve Cryptography (ECC) an asymmetric cryptography technique is used for encryption and decryption. The strength of ECC comes from the mathematical complexity of resolving the elliptic curve discrete logarithm problem [14]. ECC includes the following steps:

1. Signature generation
2. Encryption
3. Decryption
4. Signature verification

ECC is a public key cryptosystem where every user possesses two keys: public key and private key. Public key is used for encryption and signature verification while as private key is used for decryption and signature generation. Sender encrypts the message data with the help of receiver's public key and receiver decrypts the data using its private key. To verify the trustworthiness of the exchanged messages the sender signs the message by computing the hash value. To authenticate the sender's signature, the receiver should know the sender's public key. After decryption, the decrypted text is again hashed to get a hash value which will be compared to the value attached within packet header [15]. If they are equal, the data integrity is ensured and decrypted text is accepted, else it will be discarded. The system must encrypt the data so that it cannot be read without knowing the proper key. This operation imparts a certain level of security to the system because the more demanding it is to break an encrypted message the more secure the system will be. Since the data sent between each node is encrypted, it will prevent the attacker from hacking the data because one cannot decrypt the data without having proper keys. Black hole attack and Sybil attack were constructed in the network to show how the proposed system overcomes attacks, and to validate the results performance analysis was done by calculating various QoS parameters.

IV. SIMULATION RESULTS

The simulations are carried out in NS2 simulator. Table 1 represents the simulation scenario.

TABLE 1: SIMULATION PARAMETERS

Routing protocol	AODV
MAC protocol	802.11
Topography	1320 X 1032
Number of nodes	51
Packet size	1500
Traffic type	CBR
Simulation time	50 sec
Number of mobile nodes	4

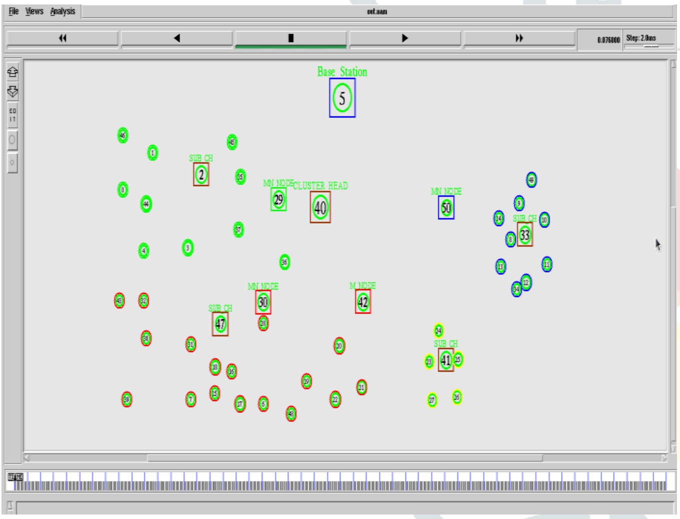


Fig 2: NAM output for simulation

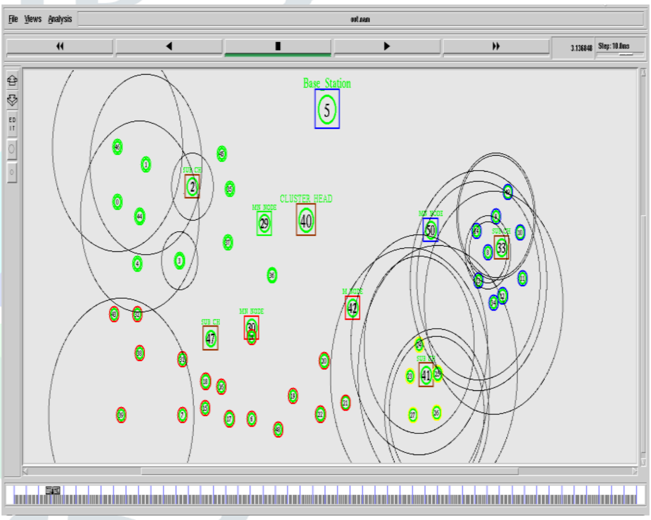


Fig 3: Data transmission

TABLE 2: SIMULATION RESULTS

Parameters	Black hole attack		Sybil attack	
	Case 1	Case 2	Case 1	Case 2
Generated packets	9086	10705	9154	10067
Received packets	8877	10459	8895	9874
PDR (%)	97.69	97.70	97.17	98.08
Average throughput (kbps)	1113.26	1319.56	1125.07	1264.30

Attack construction was done as two cases; Case one in which MN is acting malicious and case two in which child node is acting malicious. Table 2 shows the results obtained in each case. Also total remaining energy, network end-to-end delay, packet delivery ratio, TCP throughput are plotted and the plots are compared with CEETM [16], LEACH, E LEACH, M LEACH and AAWBAN [17].

Energy consumption by nodes in proposed model is less as compared to other algorithms as shown in Fig 4. The proposed system could achieve very high PDR compared to other systems as shown in Fig 5. Similarly the quality of a network connection can be measured using the TCP throughput which is the measure of rate of data that is successfully delivered over a TCP connection. As shown in Fig 6, the value of TCP throughput is high for this system when compared to others. Also the overall delay of the network is reduced significantly as shown in Fig 7.

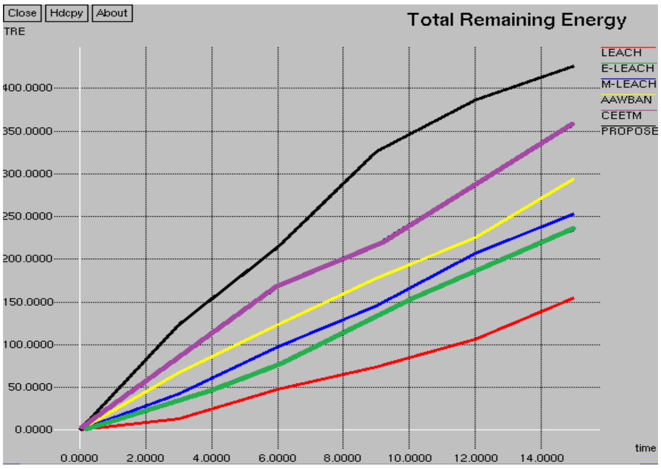


Fig 4: Comparison of total remaining energy

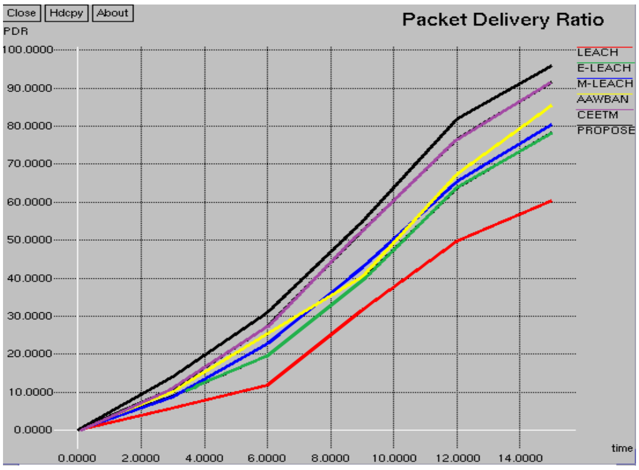


Fig 5: Comparison of PDR

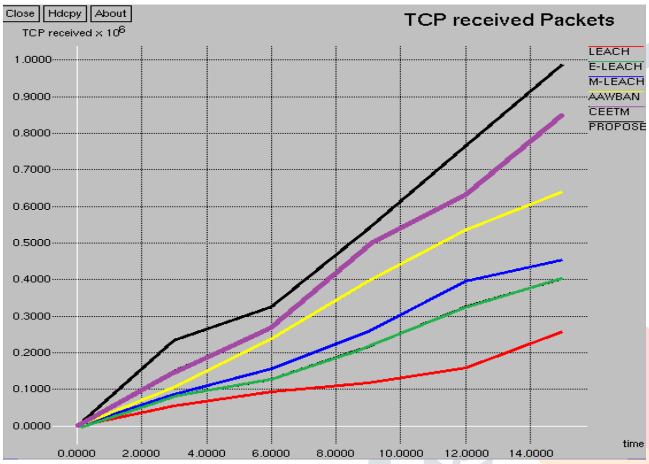


Fig 6: Comparison of TCP received packets

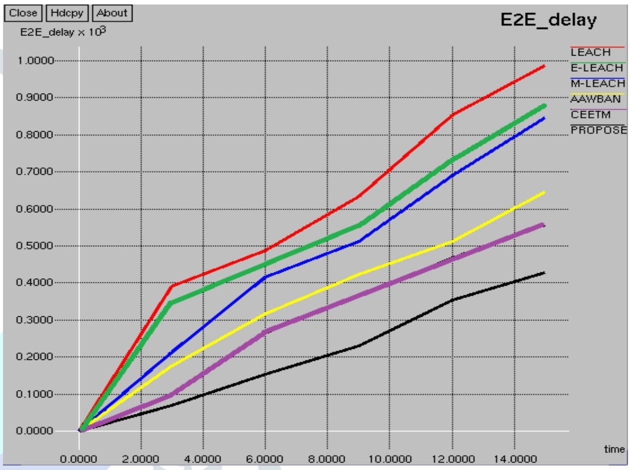


Fig 5: Comparison of end to end delay

IV. CONCLUSION

Wireless Sensor Network plays an indispensable role in several sectors. Nevertheless, there is a research gap in the area of energy efficiency and privacy issues. WSN have got several constraints of which energy efficiency and security are very important. Any system designed for WSN should be capable of providing security without affecting the network lifetime. So by this approach we could design an energy efficient and secure system which works impeccable with the resource constrained sensor networks. From the performance analysis it can be concluded that the system could achieve better PDR, increased throughput, reduced packet loss and reduced overall network delay.

REFERENCES

[1] Hybrid MAC Protocol Design for Mobile WSN ,Xin Yang , Ling Wang , Jia Su &Yanyun Gong.

[2] Elliptic Curve Cryptography (ECC) for Security in WSN ,Asha Rani Mishra,Mahesh Singh, 2012, Encryption/decryption using Elliptic Curve Cryptography, Ansah Jeelani Zargar, Mehreen Manzoor.

[3] A Review of Wireless Sensor Networks and Its Applications, Shiwei Zhang Haitao Zhang, *Proceeding of the IEEE International Conference on Automation and Logistics*,2012.

[4] A Review on Data transmission techniques for Energy Efficiency in Wireless Sensor Networks, Sandeep Kaur, Ruby Goel, *IEEE WiSPNET 2016 conference*.

[5] Heinzelman, A. Chandrakasan, H. Balakrishnan, Energy efficient communication protocol for wireless sensor networks, *Proceeding of the Hawaii International Conference System Sciences, Hawaii, January 2000*.

[6] Comparative Analysis of Clustering Protocols for Wireless Sensor Networks *International Journal of Computer Applications (0975 – 8887) Volume 115 – No. 1, April 2015* 35 Harpinder Kaur Navjot Kaur ,Sandeep Waraich.

[7] IEEE 802.15.4 Based Hybrid MAC Protocol for Hybrid Monitoring WSNs, S. Wijetunge, U. Gunawardana, R. Liyanapathirana, 2013, IEEE.

[8] hMAC: Enabling Hybrid TDMA/CSMA on IEEE 802.11 Hardware, Sven Zehl, Anatolij Zubow and Adam Wolisz, 2016.

[9] Hybrid MAC Protocol Design for Mobile Wireless Sensors Networks, Xin Yang, Ling Wang, Jia Su1 and Yanyun Gong, *IEEE Sensors*,2018.

[10] An Outline of Security in Wireless Sensor Networks: Threats, Countermeasures and Implementations, M. Yasir Malik, DOI: 10.4018/978-1-4666-0101-7.ch024.

[11] Main Types of Attacks in Wireless Sensor Networks, Teodor,Grigore Lupu, *Recent Advances in Signals and Systems*, ISSN: 1790-5109.

[12] A Secured Authentication Protocol for Wireless Sensor Networks Using Elliptic Curves Cryptography, Hsiu-Lien Yeh, Tien-Ho Chen, Pin-Chuan Liu, Tai-Hoo Kim and Hsin-Wen Wei, Sensors 2011, 11, 4767-4779.

[13] Elliptic Curve Cryptography (ECC) for Security in wireless Sensor Network, Asha Rani Mishra, Mahesh Singh, *International Journal of Engineering Research & Technology (IJERT)Vol. 1 Issue 3, May – 2011,ISSN: 2278-0181*

[14] Encryption / Decryption using Elliptical Curve Cryptography, Ansah Jeelani Zargar ,Mehreen Manzoor, *Volume 8, No. 7, July – August 2017 International Journal of Advanced Research in Computer Science ISSN No. 0976-5697* .

[15] Simulation of Wireless Sensor Network Security Model Using NS2, Nayana Hegde, Dr.Sunilkumar S.Manvi, *International Journal of Latest Trends in Engineering and Technology (IJLTET).*

[16] A Cluster Based Energy Efficient Trust Management Mechanism for Medical Wireless Sensor Networks (MWSNs), Syed Asad Hussain, Imran Raza, Mohsin Mehdi, *2018 5th International Conference on Electrical and Electronics Engineering*, 2018 IEEE.

[17] Anonymous Authentication for Wireless Body Area Networks With Provable Security, D. He; S. Zeadally; N. Kumar, J. H. Lee, in IEEE, *Systems Journal , vol.11, issue. 4, pp. 2590 – 2601, 2016.*