IMPLEMENTATION OF ZERO PROOF ALGORITHM FOR EXTENDED WIRELESS BODY SENSOR NETWORKS

Meghna Garg[1] and Manik Gupta[2]

[1]Department of Computer Engineering, Chitkara University, Baddi(H.P),India
[1]Department of Computer Engineering, Chitkara University, Baddi(H.P),India

ABSTRACT

In this research work we have proposed a machine to machine model of authentication. This model is applicable where multiple electronic devices are working continuously 24 hours for monitoring and periodically need to have authentication proving their identity and to remain the member of the network . The proposed work is implemented on health care devices. These devices form the "internet of medical devices "or simply body sensor networks connected with internet backbone. The proposed security measures include implementation of Zero proof Key based authentication scheme to protect the network from getting compromised. The efficacy of the proposed algorithm shows that the algorithm proposed is better in terms of Hardening measures.

KEYWORDS

Zero proof algorithm, Body Sensor networks, Internet of Things, Key Management Scheme

1. INTRODUCTION

Typical hardware based implementation of networks involves multiple tiny Linux embedded servers on some hardware board like wireless [1] Beaglebone Black [2] or RaspberryPi [3] that need to exchange message (e.g HL7 message) with a main server (hosted on the web)[4]. The basic mechanism is that each of these components communicate with the other device in some logical sequence by the use of RESTFul commands, for instance, the main server sends out new configurations to the embedded servers - and the servers send back data. Commands could be also issued by a human user from the main server or directly to the embedded servers also. Body Sensor network essentially will consist of components that would sense the stimuli [5] and transmit the stimuli signal to some hub, which in turn, further communicate with main server, which would realize the medical reporting system. The Body sensor must work unintended with full security. Some of the solutions to these problems are as follows:

1.1 Use a private PKI (Private Key Identifier) i.e. with custom Certification Authority and utilize mutual authentication based on public/private key pairs like SSL/TLS (Secure Socket Layer/Transport Layer Security). This has the added benefit of re-using a lot of infrastructure, so the HTTP/HTTPS/REST (Hyper Text Transfer Protocol/ Hyper Text Transfer Protocol Secure/ Representational State Transfer)"just works" as it always has been with many special changes.

1.2 By Building an Extended Key management scheme will include:

a) Digital Signature (Key usage with body sensor)
b) Key En/Decipherment (Key usage with body sensor)
c) Key Agreement (Key usage with body sensor)
d) Web Client Authentication (Extended Key Usage for cloud etc.)
e) Web Server Authentication (Extended Key Usage for server etc.)

1.3 Run a Private PKI and only allow communications between servers using a VPN (Virtual Private Network) based on PKI. Then tunnel the RESTful requests, and no others will be able to establish a VPN to one of your servers along with IP filters.

1.4 Use a Kerberos style protocol with a key distribution centre. Build a Kerberos infrastructure, including a KDC (Key Distribution Centre). Set up secure channels based on the secrets proctored by the KDC.

1.5 Use a SSH-like system (Secure Shell), public/private key pairs that only allow connections from machines whose public keys.

No matter, what we use, a highly secure and unattended security [6] measures to keep the system secure is required. Moreover, since, body sensors have constrained resources, highly efficient key management system is need of the hour. The applications are enormous of body sensor networks [23]. They can be used right from the birth of a person till his/her old age. Body sensor networks are now been developed for disease management and previous oriented healthcare. These systems may be synchronous or asynchronous in nature with multi-body platform designs and implementation may help detect motor patterns, heat stress for example. Now, these networks are also now being experimented in understanding group dynamism like understanding vital signs of a cricket team. However, it should also be noted that, some of the implication of the problems are quite grave; if link interruptions or failures occurs in "internet of medical equipment due some attack or adversity" it can lead to unwanted consequences and other medical system complications.

2. ORGANIZATION OF THE PAPER

The paper discusses the issues and problems associated related to human body sensor network. The related work section discusses various aspects of Body sensor networks from basics to its construction and challenges faced by the industry. A tabular summary of problems is also given after that and last but not least discussion and future directions are discussed after a description of a new approach for key management based on zero proof algorithm.

3. RELATED WORK

Table 1. Main Problems found in current Literature Survey[23]

S.NO	Main Problems found in current Literature Survey	
	Parameter	**Problems**
1.	Power Consumption[8]	The requirement is ultra low-powered devices.
2.	Sleep Cycle, Wakeup periods	Synchronization of sleep and cycles with stimuli and with full body sensor network.

S.NO	Main Problems found in current Literature Survey	
	Parameter	**Problems**
3.	Idle listening time	This again is issue of synchronization of all devices as per stimuli.
4.	Overhead(Control packet)	If the application of BAN is specific to particular type of stimuli. There is no need for elaborate protocol .This way we can reduce protocol stack size there by overheads.
5.	Packet collision, Retransmission[10][11]	If sudden outburst of stimuli. There is large volume of network traffic that must flow smoothly so that packets reach without delay , without collisions , retransmissions .It become challenge as routing soft components are frugal in case of WBAN .
6.	Bandwidth utilization[10][11]	Most of devices can handle small bytes, this limits the to and fro flow of data. Hence, effective use Bandwidth is critical for such devices.
7.	Seizures of stimuli[12][13]	Loading, recording the seizures of stimuli are very challenging in case of brain and when body is in movement.
8.	Storage of data collection, Time lag[4][14][6]	The need is distributed storage.
9.	Memory	Limited to store and process.
10.	Signal Integrity	Signal must maintain its coherence, shape, energy and spectrum properties and no agent must interfere /manipulate it .
11.	Signal scrambling	This can really secure signal, but at the same time this may lead to overload in terms of delay and reduced synchronization.
12.	Signal shape	No interference, no noise or distortion should be there when signal reaches control room.
13.	Key management , Key generation , Key Exchange , Key recordability	Operational resources in body sensor networks are highly restricted, incorporation of key management scheme lead to overhead, synchronization issues at the lost of security which is also essential.
14.	Area, Volume and Weight [13][15][16][17]	Unless nano, micro size is realized, there is limited scope of development in this area, as a human body must not feel burden of sensors in terms of

S.NO	Main Problems found in current Literature Survey	
	Parameter	**Problems**
		weight, area ratio and volume.
15.	Harmful effects of body sensors on human tissues and overall well being	This technology‘s side effects still need to be observed and recorded for understanding its ill effects on human body.
16.	Inert and Green technology[1]	Body sensors must not react with human tissues and affect the health due to radiation transmission of signal waves.
17.	Integration of sensor data with other clinical data.[3]	This is critical for proper working and spirit of the concept of continuous monitoring so that physician can take diagnostic decisions.
18.	Integration to main stream medical technology[3]	Body sensors network data must be interoperable for it to be used across departments and must be able to follow standards like HL7 etc.
19.	Time Synchronization	Final transmission to control room may lead to problems, challenges in terms of delay, time lag and signal may require pre and post process.
20.	Detection	In built anomaly detection, adversity identification systems are must, as these may prone to DDOS, Sybil etc, attacks.
21.	Prediction	Based on historical data, WBAN must have algorithm to predict health issues like heart attack [31] for its real success and application.

4. PROBLEM FORMULATION

Limited work has been found in literature survey for the use of “zero proof “authentication[20][22] process to check the freshness and original signature of the biometric signal transmission from machine to machine or communication of sensor to monitoring station. Since, the data flowing from these body sensors can be safely called “data streams “ and would require data streams management systems for managing such volume of data at collection station, there might be possibility that the network may come under attacks like DDOs or eavesdropping . The previous algorithms have tried to overcome this problem by having 2 phase key management systems, in which the key generation and distribution and Key exchange are done in multiple phases with fuzzy score systems or fuzzy commitment system along with time synchronization. However, these existing systems of key management have limitation in terms of their accuracy and computational cost in real time scenario in body sensor network due to inherent nature of the working.

The dynamic biometric reading may either get distorted along with the security key on the way to communication hubs. Moreover , since it is machine to machine communication , not a human – machine interaction , There is need to build a key management system that works principally

based on machine to machine authentication with seamless integration across various components of the body sensors rather than machine to human authentication process , therefore , multiple factor authentication with human interaction may not be suitable as it would lead huge time lag even if the authentication is done once in the lease time period time of the devices . However, challenge-response authentication is a family of protocols may be answer. In this protocol one party presents a question ("challenge") and another party must provide a valid answer ("response") to be authenticated, here both the parties should be machines interacting along the transmission of time series data .Hence, the protocols using “zero proof” [19][20][22]approach for authentication are more suitable for such scenarios. Therefore, for extending and improving the work in this context it is suggested that such algorithm may be used in conjunction with cryptography that makes key management scheme more secure, scalable , and reliable with low storage need to maintain low energy consumption[7][8] tradeoffs.

5. SCOPE OF THE WORK

We can finalize the scope of the work as follows, based on the conclusions drawn from tabular survey.To develop an algorithm for detecting body stimuli and synchronization of signals with key exchange scheme (fuzzy commitment) and improved scheme based on zero proof mechanism and Evaluate the security hardening and efficacy of algorithm using CVSS (Common Vulnerability Scoring System).

6. METHODOLOGY

In this section we will discuss how a body sensor network can be build which works on zero proof algorithm, a concept implementing machine to machine authentication with lowest human intervention. The section below explains a protocol in which one party(hub) can prove to another party(the verifier) that the given authentication credentials are true without conveying any information apart from the fact that the statement is indeed true. So here are the detailed steps:

6.1 Identification of heterogeneous infrastructure for building envelope around the human body for continuous monitoring.

6.1.1 HARDWARE

Body Sensors (Shimmer, Zephyrbioharness , Temperature, Wellex etc.)

6.1.2 SOFTWARE(MatLab)

6.1.3 Other Important Requirements:

a. **Sensor Observation**: Type of observation e.g. temperature, humidity, 3 axis, acceleration, gyro-fail detection etc.
b. **Data consumption model**: On demand continuous event driven time series data.
c. **Messaging**: data stream, average message rate, average length of message.
d. **Reliability**: Tolerance to packet losses.
e. **Availability**: The probability of the system availability as given time.
f. **Security**: Cryptography, data integrity, Zero proof algorithm
g. **Sensor Network**: discovery services.
h. The identity and resources registration, keeping in mind adhoc nature of nature as well as malfunction of hardware.
i. **User Type**: patent/mobile application.
j. **Persistency**
k. **Standard**:HL7 or FHIR etc.

6.2 Design of security principles for maintaining confidentiality, integrity of the signals produced by body sensor networks.

Design of key management scheme based communication type and design of 'Zero Proof' algorithm based on key management is explained.

Table 2. Communication Types between the Objects of Body Sensor Network and Key Management Requirements

S.NO	Communicating Objects	Communication Type	Key Management Requirement
1	Sensor to Sensor	Bidirectional /Direct[fig.1]	Minimal possible storage, Minimal Unnecessary exchange of Message Keys due to power constrain to maintain longer possible network life.
2	Sensor to Gateway/Hub	Bidirectional /Direct [fig.1]	Minimal possible storage in Sensor but not much issue in Gateway. Power of the Gateway/Hub is not constrained as compared to Sensor. Secure routed /tunnel communication with Keys
3	Hub/Gateway to Monitoring Server via Proxy	Bidirectional /Indirect [fig.2]	Secure routed /tunnel communication with Keys
4	Gateway to Cloud interface [9]	Bidirectional /Direct[fig.1]	Secure routed /tunnel communication with Keys

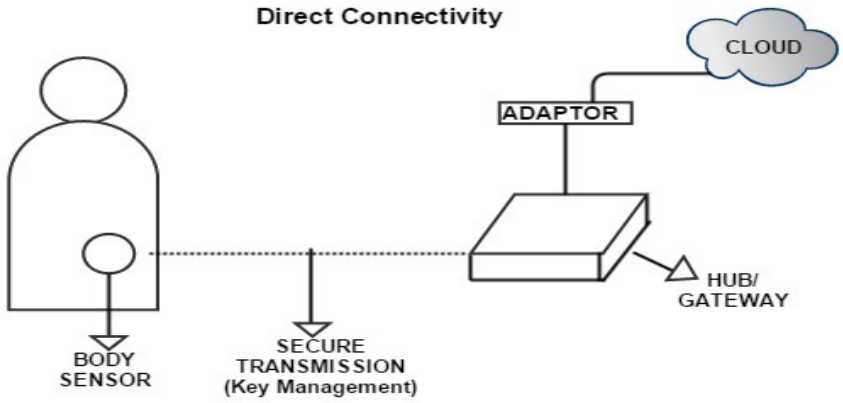

Figure 1. Direct Connectivity

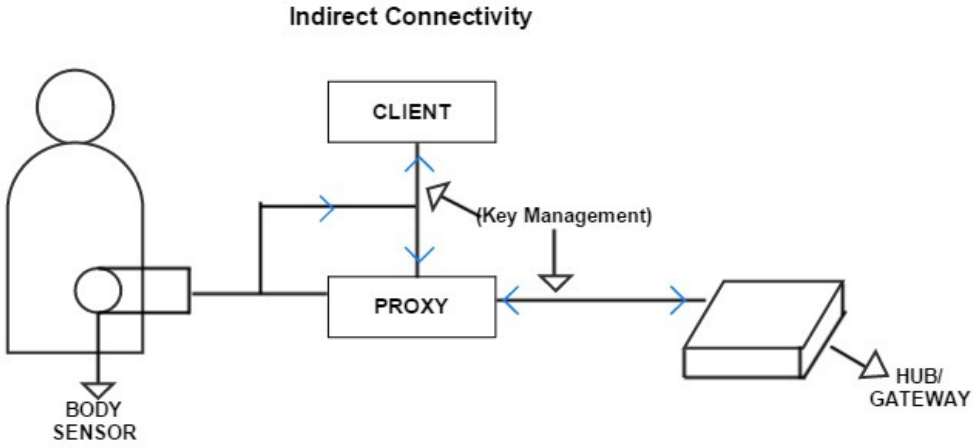

Figure 2. Indirect Connectivity

6.2.1 Key management Scheme between Sensor to Sensor Communications: Zero Proof Algorithm (S2S):

In this since, we do not want the sensors to store many keys and want to reduce the number of unnecessary exchanges between the keys, we suggest following process(Figure 3):

Let ‘sn’ be the number of Sensors.
Let ‘Ksn’ be the set of Keys Stored in each Sensor by default.
Let ‘k’ be the Primary Key, which will be used for used authentication.
Let ‘vK’ be the Verification Key to be send by Hub for verification between the two sensors at any given time.

Suppose BSN2 and BSN6 want to authenticate using the secret number "82". BSN2 takes the set of encrypted keys ‘Ksn’ out of ‘sn’ set of sensors, the sensor BSN2 runs quick sort algorithm to reach key number 82 in an unordered set of key and send a primary ‘k’ key message to BSN6.
BSN2 places the key number of 82 back in the set in the same order it was drew them (not destroying the original order).

Now it's BSN6's turn. If the BSN6 node knows Key value (82th index) then it must retrieves the 82th value (‘vK’) verification key from the key set and reveal the same value to BSN2.
If BSN2 and BSN6 retrieve different values from their indexes then they did not draw the same Key Value.

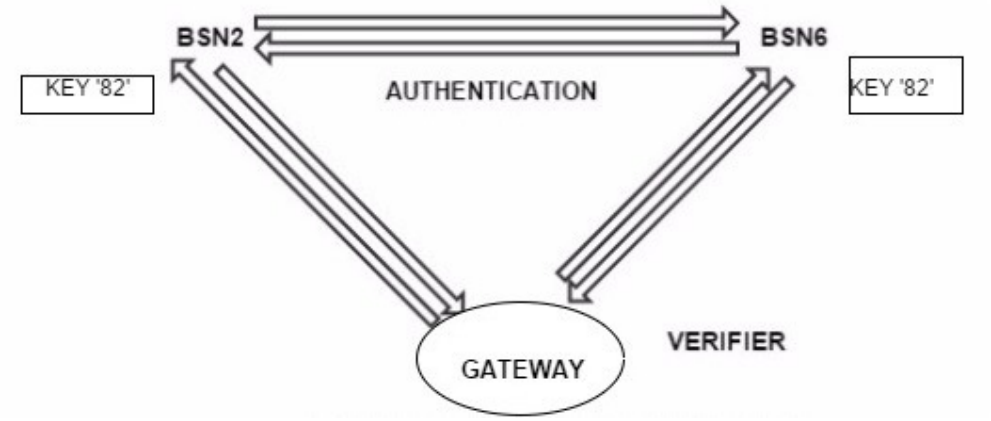

Figure 3. Sensor To Sensor Communication

6.2.2 Key management Scheme between Sensor to Gateway Communication:

Suppose BSN2 and BSN6 want to authenticate using the Key value of "82" but don't want to reveal it to one another for better security protocol. In this scenario, the key management schemes use a third party: GateWay1 [figure 4.].

GateWay1 randomly comes up with a number (any number will do) ,Let’s say 15-- and communicates it to BSN2. BSN2 then adds the Key (27) to GateWay1's number (15) and send the total (42) to BSN6.

BSN6 subtracts the Key Value (27) from the total (42) and whispers the result (15) to GateWay1.
If GateWay1 is read back his own number (15) then he can declare BSN2 and BSN6 have successfully authenticated and verified. It is assumed that GateWay1 is trustworthy always.

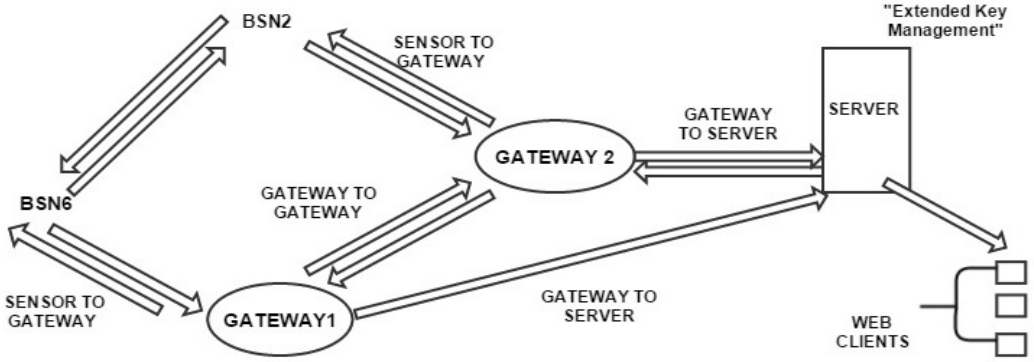

Figure 4.

6.2.3 Key management Scheme between Gateway to Monitoring Server via Proxy:

Assuming that [Gateway2] has a secret key x and public key y = gx. (Here we assume that g generates a group G of size p, for large prime p.) [Gateway2] wants to convince BSN6 [Monitoring Server] that it knows x without revealing x. This is a typical example of an authentication/identification protocol.

[Gateway2] generates 'a' new random value r, and sends a = gr to [Monitoring Server]. [Monitoring Server] replies with a random k-bit challenge c, and then [Gateway2] sends z = cx+rmodp to [Monitoring Server]. [Monitoring Server] accepts if gz=yca.

This is a special "challenge-response" type of protocol, also known as a Σ-protocol. The concrete protocol above was proposed by Schnorr. It is not completely ZK by itself, but it is zero knowledge if we assume that [Monitoring Server]is honest (c is really chosen randomly).Hence it is modified variant proposed for body sensor networks.

The proof of this fact: we show by using simulation, that [Monitoring Server] can create (a′,c′,z′) that comes from the same distribution as the real protocol view (a,c,z), but without knowing the secret key x. The trick is that we allow BSN6 to choose c′ and z′ first and then to choose a so that the verification equation will accept.

Namely, the random number generator creates random c′ and z′, and then chooses a′=gz′/yc′. Clearly, this triple (a′,c′,z′) satisfies the verification. Moreover, in the original protocol (a,c,z) is a tuple of random values from (G,{0,1}k,Zp) modulo the verification requirement. But so is the simulated triple.

That "honest-verifier zero knowledge" proof can be made fully zero knowledge by (basically, letting Monitor to "commit" to 'c' before he reads 'a' - the actual solution. Since, the communication is via proxy that allows http or https , the authentication mechanism may optionally use sockets else default protocol for authentication.

6.2.4 Extended Key management Scheme between Gateway to Cloud interface

In this case Restful api, will be interacting and authentication can be done with exchange of response challenge mechanism same as in Gateway to Monitoring Server, via Proxy [Fig 4.]

6.3.Evaluation of the implementation of security, ecosystem with respect to key management.

Present study focuses only on extended body sensor network assertion levels. In order to understand the vulnerabilities at assertion level and to evaluate the hardness of our proposed Zero proof algorithm [21][19] hardening we carried out proposed attacks namely – Network Wire trap Attack. Hardness of the proposed protocol was evaluated by Common Vulnerability Scoring System (CVSS). [18]

6.2.5 CVSS score without hardening

The attack under study was simulated and CVSS score before hardening was calculated in order to objectively measure vulnerability of the system. Before hardening the status of network was kept as under: [Table 3]

Table 3. CVSS score without Hardening

Base Metric	**Metric Value**	
Access Vector	Network (N)	1
Access Complexity	Low (L)	.71
Authentication	Multiple (M)	.45
Confidentiality Impact	Complete (C)	.660
Integrity Impact	Complete (C)	.660
Availability Impact	Partial (P)	.275

Availability Impact Partial (P) .275

Accordingly attacks were carried out remotely, with low complexity and requiring multiple authentication. As predicted the confidentiality and integrity of services were completely compromised while availability was partially compromised. Base score before hardening was calculated.

Base Score = [(.6 * impact) + .4 (exploitability) – 1.5] * f (impact) (1)
Impact = 10.41 * [1-(1- ConfImpact) * (1- IntegImpact) * (1- AvailImpact)] (2)
Exploitability = 20 * Access Vector * Access Complexity * Authentication (3)
From Equation (2)
Impact = 10.41 [1 – (1 - .660) * (1-.660) * (1-.275)]
= 10.41 [1- (.08381)]
= 10.41 [.91619]
= 9.53
From Equation (3)
Exploitability = 20 * 1 * 0.71 * 0.45
= 6.39
From Equation (1)
Base Score = [0.6 (9.53) + 0.4 (6.39) – 1.5] * 1.176
= 8

So, CVSS before hardening was 8, which is fairly high on 0 – 10 point CVSS scale [0 indicating completely secure network and 10 indicating completely vulnerable network].

6.2.6 CVSS score after hardening

Hardening of the network was carried by Zero proof and again the three attacks were simulated but under similar conditions. For the purpose of calculating CVSS the network settings were kept as below [Table 4.]

Table 4. CVSS score after hardening

Base Metric	**Metric Value**	
Access Vector	Network (L)	1
Access Complexity	Low (L)	0.71
Authentication	Multiple (M)	0.45
Confidentiality Impact	Partial (P)	.275
Integrity Impact	Partial (P)	.275
Availability Impact	None (N)	0.0

From equation (2)
Impact = 10.41 * [1 – (1 – 0.275) * (1 – 0.275) * (1 – 0.0)]
= 4.9

From Equation (3)
Exploitability = 20 * 1 * 0.71 * 0.45 = 6.39

From equation (1)
Base Score = [0.6 (4.9) + 0.4 (6.39) – 1.5] * 1.176
= [(2.9 + 2.55) – 1.5] * 1.176
= [5.45 -1.5] * 1.176
= 4.7

The CVSS score before (8) and after (4.7) hardening indicate that hardening has been effective. The orientation of these attacks was such that they appeared to be from a remote location (network), of low complexity and access required multiple verifications. In an unprotected scenario it was found that network confidentiality and integrity was completely compromised while network availability was partially compromised. Similar types of attacks were carried out after hardening with Zero proof Algorithm [19][20][21][22] and it was found that network confidentiality and integrity was only partially and not completely comprised, while availability was totally protected. This was confirmed with CVSS. [Figure 5] shows CVSS before and after hardening.

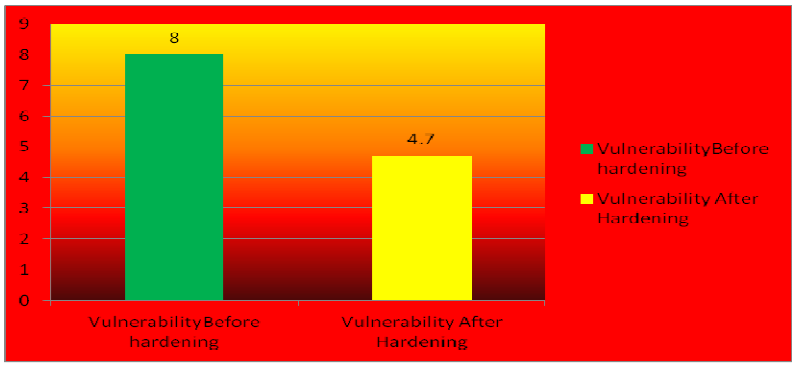

Figure 5. CVSS before and after hardening.

Figure 6 and Figure 7 provide and insight into comparison of security and vulnerability of the network before and after hardening.

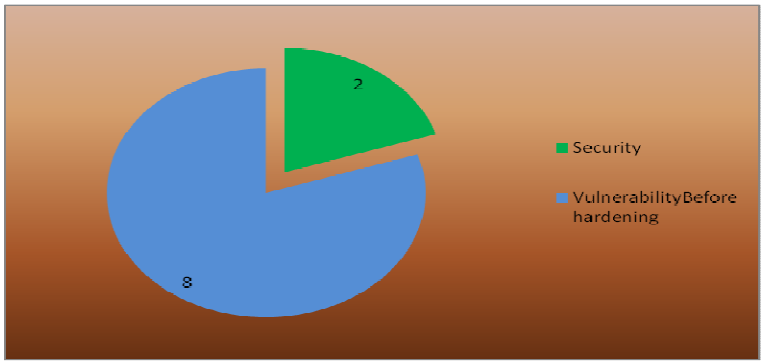

Figure 6.CVSS comparison between security and vulnerability before hardening.

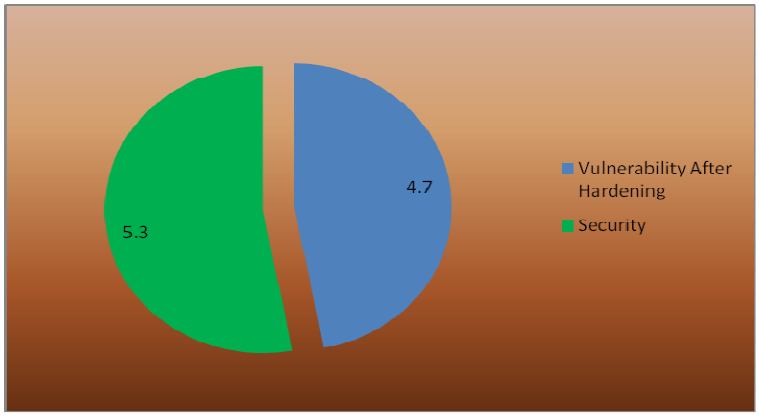

Figure 7.CVSS comparison between security and vulnerability after hardening.

7. CONCLUSIONS

In summary , we can state that , based on the communication type and constrains of the Body sensor networks a suitable modified version zero proof algorithms have been implemented in five ways : 1) Sensor to sensor 2) Sensor to Gateway 3) Gateway to Gateway 4) Gateway to Monitoring Station 5) Monitoring Station to cloud interface . Care has been taken in case of Sensor to sensor communication to keep the number of rounds lows and we have used simple array and selecting algorithm to retrieve keys and match. The storage requirement in case remain low and similar approach is applied when sensor to gateway communication occurs, a case when need for third party verification arises. In case of Gateway to Gateway, Gate Way to Monitoring communication, when power and storage is of no constrain, we have used more variant of the zero proof algorithm where security is enhanced. When a client simply transmits the original password to the server, which re-computes the password hash and compares it to the stored value.The problem remains the same, the server has learned my clear text password .Hence, we can only wish that servers will never be compromised, this is avoided by our key management scheme in case of server and cloud interactions with the sensor authentication process. Our scheme is a basically a commitment scheme , that allows one party to 'commit' to a given message while keeping it secret, and then later 'open' the resulting commitment to reveal what's inside.

8. FUTURE SCOPE

The security of most of the zero-knowledge proof of identity protocols is based on complex mathematical algorithms and requires heavy computations for both parties normally , but here a simplified version of the zero proof algorithm was used in case of sensor to sensor communication , that avoided large number of round. For future scope we suggest polynomial co-efficients mat be used for proof, instead of normal multiplication, addition operations as it would increase the complexity but over head may remain same.

ACKNOWLEDGEMENTS

I would like to take this opportunity to thank my guide Manik Gupta and my parents for helping me in the research study.

REFERENCES

[1] Naveen, Chilamkurti, Zeadally Sherali, Jamalipour Abbas, and Das Sajal K. "Enabling Wireless Technologies for Green Pervasive Computing." EURASIP Journal on Wireless Communications and Networking 2009 (2010)

[2] Lui, K.W.; Murphy, O.H.; Toumazou, C., "A Wearable Wideband Circularly Polarized Textile Antenna for Effective Power Transmission on a Wirelessly-Powered Sensor Platform," Antennas and Propagation, IEEE Transactions on , vol.61, no.7, pp.3873,3876, July 2013

[3] Clifton, L.; Clifton, D.A.; Pimentel, M.A.F.; Watkinson, P.J.; Tarassenko, L., "Predictive Monitoring of Mobile Patients by Combining Clinical Observations With Data From Wearable Sensors," Biomedical and Health Informatics, IEEE Journal of , vol.18, no.3, pp.722,730, May 2014

[4] Khan, Tareq Hasan, and Khan A. Wahid. "An advanced physiological data logger for medical imaging applications." EURASIP Journal on Embedded Systems 2012, no. 1 (2012): 1-14.

[5] Alotaiby, Turkey N., Saleh A. Alshebeili, Tariq Alshawi, Ishtiaq Ahmad, and Fathi E. Abd El-Samie. "EEG seizure detection and prediction algorithms: a survey." EURASIP Journal on Advances in Signal Processing 2014, no. 1 (2014): 183

[6] Le, T.Q.; Changqing Cheng; Sangasoongsong, A.; Wongdhamma, W.; Bukkapatnam, S.T.S., "Wireless Wearable Multisensory Suite and Real-Time Prediction of Obstructive Sleep Apnea Episodes," Translational Engineering in Health and Medicine, IEEE Journal of , vol.1, no., pp.2700109,2700109, 2013.

[7] Awad, A.; Hussein, R.; Mohamed, A.; El-Sherif, A.A., "Energy-aware cross-layer optimization for EEG-based wireless monitoring applications," Local Computer Networks (LCN), 2013 IEEE 38th Conference on , vol., no., pp.356,363, 21-24 Oct. 2013.

[8] Kaur, Jasdeep, and Sandeep Singh Gill. "QoS based energy efficient key management in body sensor networks." In Medical Imaging, m-Health and Emerging Communication Systems (MedCom), 2014 International Conference on, pp. 14-19. IEEE, 2014.

[9] Misra, S.; Das, S.; Khatua, M.; Obaidat, M.S. "QoS-Guaranteed Bandwidth Shifting and Redistribution in Mobile Cloud Environment", Cloud Computing, IEEE Transactions , On page(s): 181 - 193 Volume: 2, Issue: 2, April-June 2014

[10] Xia, Lingli, Stephen Redfield, and Patrick Chiang. "Experimental characterization of a UWB channel for body area networks." EURASIP Journal on Wireless Communications and Networking 2011 (2011): 4.

[11] Sana, Ullah, Higgins Henry, Islam SM Riazul, Khan Pervez, and Kwak Kyung Sup. "On PHY and MAC performance in body sensor networks." EURASIP Journal on Wireless Communications and Networking 2009 (2009).

[12] Alotaiby, Turkey N., Saleh A. Alshebeili, Tariq Alshawi, Ishtiaq Ahmad, and Fathi E. Abd El-Samie. "EEG seizure detection and prediction algorithms: a survey." EURASIP Journal on Advances in Signal Processing 2014, no. 1 (2014): 183.

[13] McDowell, K.; Chin-Teng Lin; Oie, K.S.; Tzyy-Ping Jung; Gordon, S.; Whitaker, K.W.; Shih-Yu Li; Shao-Wei Lu; Hairston, W.D., "Real-World Neuroimaging Technologies," Access, IEEE , vol.1, no., pp.131,149, 2013 .

[14] Costlow, T., "Camera phone bans expected," Distributed Systems Online, IEEE , vol.5, no.2, pp.5/1,5/3, Feb. 2004

[15] Koulali, Mohammed-Amine, Abdellatif Kobbane, Mohammed El Koutbi, Hamidou Tembine, and Jalel Ben-Othman. "Dynamic power control for energy harvesting wireless multimedia sensor networks." EURASIP Journal on Wireless Communications and Networking 2012, no. 1 (2012): 1-8.

[16] Al Ameen, Moshaddique, Niamat Ullah, M. Sanaullah Chowdhury, SM Riazul Islam, and Kyungsup Kwak. "A power efficient MAC protocol for wireless body area networks." EURASIP Journal on Wireless Communications and Networking 2012, no. 1 (2012): 1-17.

[17] Begonya, Otal, Alonso Luis, and Verikoukis Christos. "Design and analysis of an energy-saving distributed mac mechanism for wireless body sensor networks." EURASIP Journal on Wireless Communications and Networking 2010 (2010).

[18] www.first.org/cvss

[19] Ibrahem, M.K., "Modification of Diffie-Hellman key exchange algorithm for Zero knowledge proof," Future Communication Networks (ICFCN), 2012 International Conference on , vol., no., pp.147,152, 2-5 April 2012.

[20] Jaafar, A.M.; Samsudin, A., "Visual Zero-Knowledge Proof of Identity Scheme: A New Approach," Computer Research and Development, 2010 Second International Conference on , vol., no., pp.205,212, 7-10 May 2010.
[21] Wu, Huixin; Wang, Feng (2014). "A Survey of Noninteractive Zero Knowledge Proof System and Its Applications". The Scientific World Journal 2014: 1–7.
[22] Sahai, Amit; Vadhan, Salil (1 March 2003). "A complete problem for statistical zero knowledge" (PDF). Journal of the ACM 50 (2): 196–249.
[23] Meghna Garg and Manik Gupta, "Technical Issues and Challenges in Building Human Body Sensor Networks" International Journal of Advanced Computer Science and Applications(IJACSA), 6(6), 2015.

Authors

Manik Gupta is Assistant Professor in the Department of Computer Science at Chitkara University, Himachal Pradesh, India. He has a good number of publications in the field of wireless sensor networks in various international conferences and journals of good repute. He had been awarded for Best Research Paper, in December, 2010. He also worked as Software Developer for one year after completing his Bachelors in Engineering and as Consultant in LSI, Research and Development. He also remained a regular columnist of column "Manik's Tech Tonics" in the newspaper- "Student Age". His research area is Security, Energy Efficiency, Fault Tolerance, Fault Revoking, Coverage, Connectivity and Mobility in Wireless Sensor Networks an Body Area Sensor Networks.

Meghna Garg is currently persuing Integrated METech from Chitkara University and have keen interest in Human Body Sensor networks and other related technologies