International Journal of Research
Available at https://pen2print.org/index.php/ijr/
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 22
November 2018

A Cluster Head Rotation method Based Energy Efficient Trust Management Mechanism for Wireless Sensor Networks (MWSNs)

[1]Sneha K S & [2]Liston Deva Glindis

[1]Master Of Engineering, Dept. of CSE, Dhanalakshmi Srinivasan College Of Engineering, Coimbatore, India, Mail Id:- snehaks012@gmail.com

[2]Assistant Professor, Dept. of CSE, Dhanalakshmi Srinivasan College Of Engineering, Coimbatore, India, Mail Id: - listong@dsce.ac.in

Abstract

This paper presents an energy efficient trust management model for securing lifesaving information with optimal power/energy consumption by sensor nodes. The proposed model is a cluster based three tier-architectures where first tier records the first-run configuration of the nodes. The second tier secures the data between the nodes, and the third tier ensures energy efficiency by calculating energy consumption at every level and rotates cluster head among the nodes. The difficult task of energy efficiency is achieved through robust algorithms, which configure the nodes and train the network using a machine learning technique. The simulation results show smooth functioning of the network with less energy consumption. The proposed scheme performs better than Anonymous Authentication for Wireless Body Area Networks with Provable Security (AAWBAN) in terms of computational overhead, energy consumption, and throughput and data drop rate.

Keywords: - AAWBAN, WSNs GPS, RFID.

1. INTRODUCTION

The advancements in wireless communication technologies enabled large scale wireless sensor networks (WSNs) deployment. Due to the feature of ease of deployment of sensor nodes, wireless sensor networks (WSNs) have a vast range of applications such as monitoring of environment and rescue missions. Wireless sensor network is composed of large number of sensor nodes. The event is sensed by the low power sensor node deployed in neighborhood and the sensed information is transmitted to a remote processing unit or base station. To deliver crucial information from the environment in real time it is impossible with wired sensor networks whereas wireless sensor

e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 22
November 2018

networks are used for data collection and processing in real time from environment. The ambient conditions in the environment are measured by sensors and then measurements are processed in order to assess the situation accurately in area around the sensors. Over a large geographical area large numbers of sensor nodes are deployed for accurate monitoring. Due to the limited radio range of the sensor nodes the increase in network size increases coverage of area but data transmission i.e. communication to the base station (BS) is made possible with the help of intermediate nodes. Depending on the different applications of wireless sensor networks they are either deployed manually or randomly. After being deployed either in a manual or random fashion, the sensor nodes self-organize themselves and start communication by sending the sensed data. These sensor networks are deployed at a great pace in the current world. Access to wireless sensor networks through internet is expected within 10-15 years. There is an interesting unlimited potential in this wireless technology with various application areas along with crisis management, transportation, military, medical, natural disaster, seismic sensing and environmental. There are two main applications of wireless sensor networks which can be categorized as: monitoring and tracking. The use of different wireless devices like cell phones, GPS devices, laptops, RFID and other electronic devices have become more pervasive, cheaper and important in today's life. The demand for communication and networking among these various wireless devices has been increased for different applications. Wireless sensor networks from this point of view are the latest trend. Ad Hoc Network (MANET) that is connected by wireless links is a self-configuring network of mobile nodes. The devices freely move in any direction and links among these devices are changed frequently. A cooperative network organized by collection of sensor nodes is a wireless sensor network. Both of these networks fall into the category of infrastructure less wireless networks as they do have any requirement regarding infrastructure during the deployment. Wireless Local Area Networks (WLANs) and cellular networks fall into the other category of wireless networks that require infrastructure during their deployment. Routing of information differentiate these networks from other ad-hoc networks. The study of wireless sensor network is done by performing simulation that can help in

e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 22
November 2018

better understanding of behavior of various routing protocols. Diverse characteristics of Medical Wireless Sensor Networks (MWSNs) facilitate remote monitoring of patients in healthcare applications. A brief exploration of several health care projects (AlarmNet, MobiCare, MediSN, UbiMone) reveals that provision and maintenance of reliable security against several attacks is a major requirement for providing immediate treatment to the patients. An integration of health care service systems with the cloud computing architecture employs physiological sensing devices that are capable of continuous monitoring and raising alarm for emergency situations. Such a successful operation is guaranteed only when all nodes function in a trustworthy manner. Trust among the nodes ensures robustness, reliability, and verification. Several trust management mechanisms have been proposed for healthcare systems.

2. RELATED WORK

Proposed system

This paper presents an energy efficient trust management model for securing life-saving information with optimal power/energy consumption by sensor nodes. The proposed model is a cluster based 3 tiers – architecture where first tier records the first-run configuration of the nodes. The second tier secures the data between the nodes, and the third tier ensures energy efficiency by calculating energy consumption at every level and rotates cluster head among the nodes. The difficult task of energy efficiency is achieved through a robust algorithm, which configures the nodes and trains the network using a machine learning technique. The simulation results show smooth functioning of the network with less energy consumption. The proposed scheme performs better than Anonymous Authentication for Wireless Body Area Networks with Provable Security (AAWBAN) in terms of computational overhead, energy consumption, and throughput and data drop rate. In proposed model, for every entry AVP is encrypted during the first execution. The encryption of the AVP is performed by adding another tag consisting of node ID and this can be represented for first tier architecture-node registration. For second tier architecture clustering, in order to divide the computation overhead over the network we have proposed clusters of closely related nodes based on the distance and signal strength. Each cluster is headed by a cluster head (CH) which takes most of the computation and stores the configuration file of all the nodes. When

e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 22
November 2018

energy consumption goes beyond the set limit the cluster head configuration is sent to another node. This divides the overhead and maintains energy efficiency. At last, for third tier architecture-energy efficiency, energy efficiency is the overall requirement and the proposed algorithm keeps on calculating it and when energy consumption reaches the defined limit a new CH is assigned. New CH assignment depends upon the trust value of the node. In order to become a CH the node has to achieve a certain level of trust. This is achieved by ranking of rating by other nodes and assignment of lower and upper weight limits depending on a successful communication log.

ADVANTAGES

- For overall requirement, it maintains energy efficiency.

DISADVANTAGES

3. QoS (Quality of Service is low).
4. **IMPLEMENTATION**

WSN have the following distinctive characteristics:

They can be deployed on large scale. These networks are scalable; the only limitation is the bandwidth of gateway node. Wireless sensor networks have the ability to deal with node failures. Another unique feature is the mobility of nodes. They have the ability to survive in different environmental surroundings. They have dynamic network topology. Further developments in this technology have led to integration of sensors, digital electronics and radio communications into a single integrated circuit (IC) package. Generally wireless sensor network have a base station that communicates through radio connection to other sensor nodes.

Sensor node components

There are various sensor nodes having capabilities regarding power of microcontroller, radio and capacity of memory. Despite of the variances it can be said that there are four basic sub- systems of sensor nodes; computing subsystem, sensing subsystem, power subsystem and communication subsystem.

Controlling Component

In order to control the components of the sensor nodes and perform the required computations this subsystem is responsible for it. There are two sub-units, storage unit and processor unit. There are different operational modes of processors in sensor nodes. They are either Idle, Active or in Sleep modes. In order to preserve power this is important, so processor operates when required.

Communication Component

The sensor nodes due to this component interact with the base station and to the

other nodes. Usually this subsystem is a radio of short range but other fields has also been explored like ultrasound, infrared communication and inductive fields. The advantage of radio frequency communication for sensor nodes is that it is not limited by line of sight and low-power radio transceivers with data-rates and ranges depending on the applications are easily implemented with the help of current technology.

Power Component

Power is supplied to sensor nodes by this sub-system in which a battery is contained. Every aspect of the network regarding communication algorithms, sensing devices, localization algorithms should be efficient in terms of energy usage because replacement or recharging of battery is unfeasible in case where large numbers of sensor nodes are deployed. For recharging of battery onsite a power generator should be included.

Sensing Component

In this sub-system the physical phenomena is converted to electrical signals by sensor transducers. So the outside world is linked to this subsystem. Sensors may have analog or digital output. There should be an analog to digital converter (ADC) increase if output is analog. In general wireless communication is classified into two main categories as mentioned before. These two categories are infrastructure based and infrastructure less and further infrastructure less networks are divided into two groups which are WSNs and MANETs. The two networks are equivalent but built for different purposes. Both groups of wireless networks are self-organizing networks where nodes are connected by wireless links, can move freely and the topology of the network changes constantly.

5. PROCESS OF APPLICATION

NS is an event driven network simulator developed at UC Berkeley that simulates variety of IP networks. It implements network protocols such as TCP and UPD, traffic source behavior such as FTP, Telnet, Web, CBR and VBR, router queue management mechanism such as Drop Tail, RED and CBQ, routing algorithms such as Dijkstra, and more. NS also implements multicasting and some of the MAC layer protocols for LAN simulations. The NS project is now a part of the VINT project that develops tools for simulation results display, analysis and converters that convert network topologies generated by well-known generators to NS formats. Currently, NS (version 2) written in C++ and OTcl (Tcl script language with Object-oriented extensions developed at

MIT) is available. This document talks briefly about the basic structure of NS, and explains in detail how to use NS mostly by giving examples. As shown in Figure 1, in a simplified user's view, NS is Object-oriented Tcl (OTcl) script interpreter that has a simulation event scheduler and network component object libraries, and network setup (plumbing) module libraries (actually, plumbing modules are implemented as member functions of the base simulator object). In other words, to use NS, you program in OTcl script language. To setup and run a simulation network, a user should write an OTcl script that initiates an event scheduler, sets up the network topology using the network objects and the plumbing functions in the library, and tells traffic sources when to start and stop transmitting packets through the event scheduler. The term "plumbing" is used for a network setup, because setting up a network is plumbing possible data paths among network objects by setting the "neighbor" pointer of an object to the address of an appropriate object.

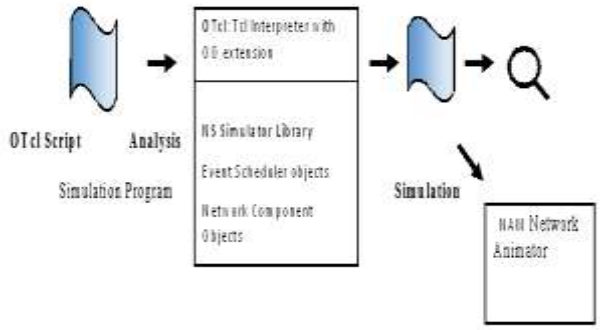


Figure 1 Simplified User's View of NS

Another major component of NS beside network objects is the event scheduler. An event in NS is a packet ID that is unique for a packet with scheduled time and the pointer to an object that handles the event. In NS, an event scheduler keeps track of simulation time and fires all the events in the event queue scheduled for the current time by invoking appropriate network components, which usually are the ones who issued the events, and let them do the appropriate action associated with packet pointed by the event.

6. SIMULATION RESULTS

Figure 2 Network Constructions in NAM Window

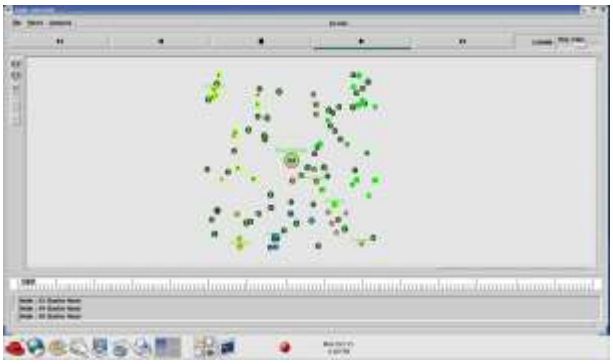


Figure 3 Cluster Head Selection and Data Transmission

e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 22
November 2018

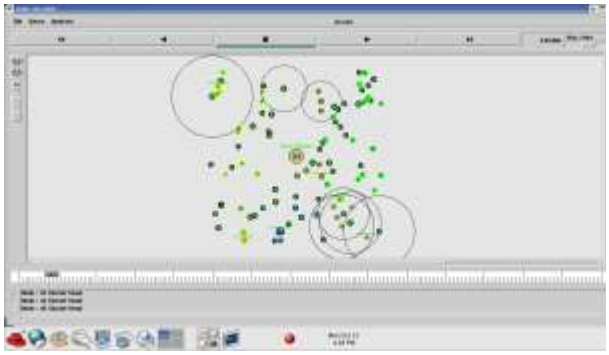


Figure 4 Total Remaining Energy Calculation of the Network

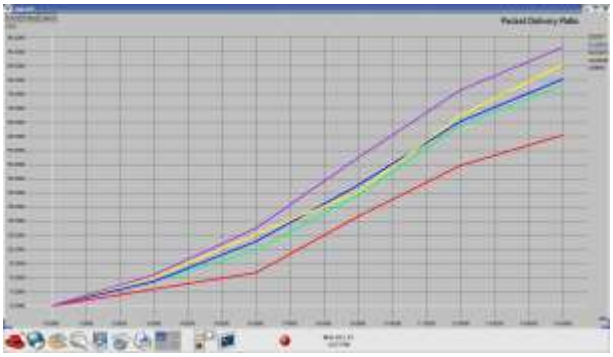


Figure 7 Average Remaining Energy Calculation of the Network

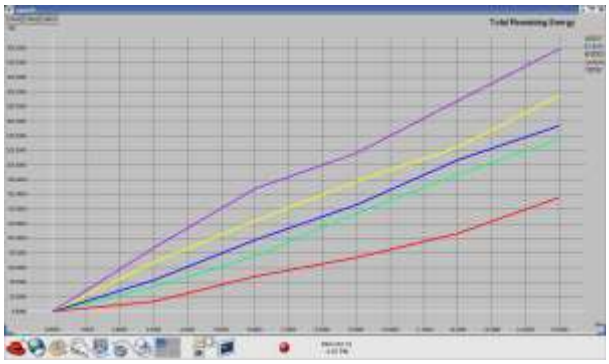


Figure 5 Total TCP Received Packet Calculation of the Network

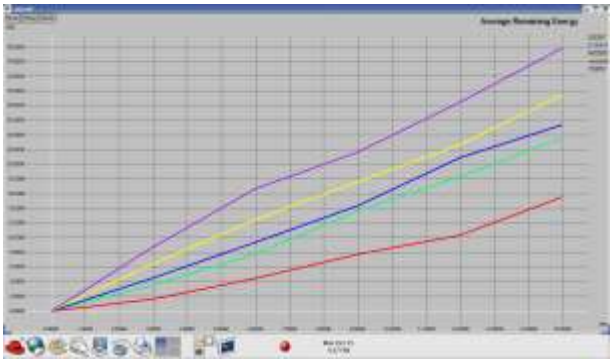


Figure 8 TCP Throughput Calculation of the Network

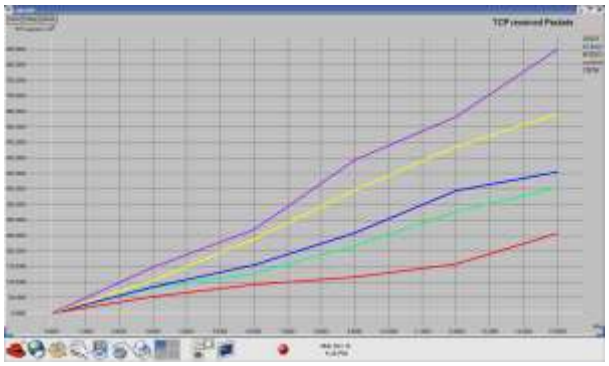


Figure 6 Packet Delivery Ratio Calculation of the Network

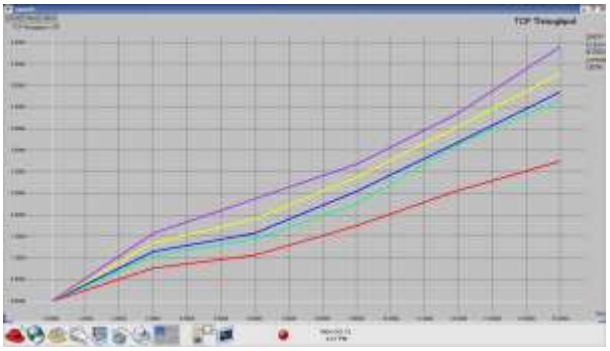
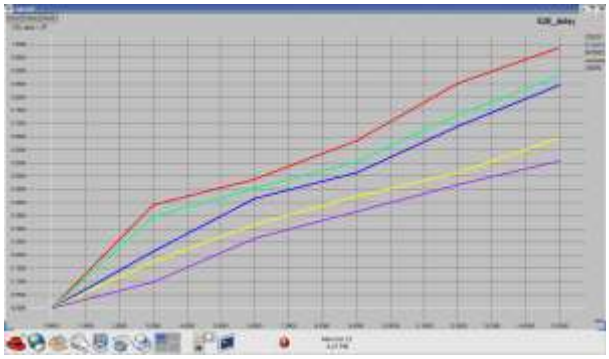


Figure 9 End to End Delay Calculation of the Network

e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 22
November 2018



7. CONCLUSION

Energy efficiency is an important concern in resource sensitive healthcare sensor based devices. Due to the neglect of this vital parameter several latest technologies have failed to address trust management issues with optimal energy consumption. The proposed model with its 3-tier architecture and efficient cluster-based computation allowed the network to perform better in terms of computational overhead, throughput, energy consumption and data drop rate. Trust among nodes is achieved by registration through AVP values and then re-clustering of nodes allows distribution of computation overhead. This results in a comprehensive energy efficient solution.

REFERENCES

[1] F. Ullah, A. H. Adullah, M. Q. Jan, and K. N. Qureshi, "Patient data prioritization in the cross-layer designs of wireless body area network," Journal of Computer Networks and Communications, vol. 2015, Article ID 516838, 21 pages, 2015. doi: 10.1155/2015/516838 2015.

[2] Gu Xiang, Qiu Jianlina, Wang Jina, "Research on Trust Model of Sensor Nodes in WSNs", in International Workshop on Information and Electronics Engineering (IWIEE), pp.45-57, 2012.

[3] D. He, C. Chen, S. Chan, J. Bu, and A. V. Vasilakos, "ReTrust: Attack-resistant and lightweight trust management for medical sensor networks," IEEE Transactions on Information Technology in Biomedicine, vol. 16, no. 4, pp. 623-632, 2012.

[4] M. Somasundaram and R. Sivakumar, "Game Theory Based Security in Wireless Body Area Network with Stackelberg Security Equilibrium". The Scientific World Journal, vol. 2015, Article ID 174512, 9 pages, 2015. doi:10.1155/2015/174512.

[5] X. Qi, K. Wang, A. Huang, H. Hu, and G. Han, "MAC protocol in wireless body area network for mobile health: a survey and an architecture design," International Journal of Distributed Sensor Networks, vol. 11, issue 10. 2015.

[6] C. Hu, X. Cheng, F. Zhang, D. Wu, X. Liao, and D. Chen, "OPFKA: Secure and efficient ordered-physiological-feature-based key agreement for wireless body

area networks," in INFOCOM 2013 Proceedings IEEE, 2013, pp. 2274-2282.

[7] Y. S. Lee, E. Alasaarela, and H. Lee, "Secure key management scheme based on ECC algorithm for patient's medical information in healthcare system," in The International Conference on Information Networking 2014 (ICOIN2014), 2014, pp. 453-457.

[8] P. Picazo-Sanchez, J. E. Tapiador, P. Peris-Lopez, and G. SuarezTangil, "Secure publish-subscribe protocols for heterogeneous medical wireless body area networks," Sensors, vol. 14, issue 12, pp. 22619-22642, 2014.

[9] P. Porambage, C. Schmitt, P. Kumar, A. Gurtov, and M. Ylianttila, "Pauthkey: A pervasive authentication protocol and key establishment scheme for wireless sensor networks in distributed iot applications," International Journal of Distributed Sensor Networks, vol. 2014, 2014.

[10] S. B. Othman, A. A. Bahattab, A. Trad, and H. Youssef, "Secure data transmission protocol for medical wireless sensor networks," in IEEE 28th International Conference on Advanced Information Networking and Applications, 2014, pp. 649-656.