Big Data and Computing Visions

www.bidacv.com

Big. Data. Comp. Vis. Vol. 2, No. 2 (2022) 90–94.

Paper Type: Original Article

The Role of Wireless Sensor Networks in the Modern Landscape: A Concise Examination

Salwa El-Morsy*

Department of Mathematics, College of Science and Arts, Al-Badaya, Qassim University, Saudi; s.elmorsy@qu.edu.sa.

Citation:

El-Morsy, S. (2022). The role of wireless sensor networks in the modern landscape: a concise examination. *Big data and computing visions, 2*(2), 90-94.

Received: 16/11/2021 Reviewed: 22/12/2021 Revised: 13/01/2022 Accept: 23/02/2022

Abstract

Wireless sensor networks are fast process of connection in part such as agriculture, healthcare, environmental monitoring, security, and manufacturing and also it thesaurus and measure physical signals and it also have wireless communication. Wireless sensors also can track the appliances; it is an automatic control of devices. It works as an investigation of types and application of wireless sensors in the ground and home. In this paper we have presented sort study on WSN applications.

Keywords: Wireless sensor, Networks, Smart home appliances.

1 | Introduction

There have been an improvement in automation of devices and processes in our surroundings. Some key components jam these intelligent systems and here some sensors detect and measure the physical quantity [1]. It provides some information on system operate. sensor measure various position of parameters such as temperature, and light intensity [2]. The wired system sensors have some drawbacks, such as it has some difficulty in installation and maintenance and wired sensors are unsuitable for remote terrain [3]. Some of the sensor systems are wired; the data will be recorded and monitored, processed and used to control various components the wireless sensors are very easy to handle in deployment, installation and maintenance [4]. The wireless sensors are have more important role in home appliances and health, agriculture and wireless sensors have different challenges involved [5]. The large number of keys should be managed in order encrypt and authentic all sensitive data [6]. The objective is to dynamically establish and maintain secure channels among communicating equal, the key management solutions use administrative for security purpose [7]. Session keys are used in pair-wise to secure communication channel between two nodes they are in direct and indirect communication or in group key.

The dynamical key management schema having the appropriate network with multi-tier hierarchical architecture deployed in a hostile environment [8]. The hierarchical network of bottom tier contains

Corresponding Author: s.elmorsy@qu.edu.sa

https://doi.org/10.22105/bdcv.2022.334376.1080

cluster of sensor nodes, the clusters contains many low-end nodes [9]. In the hostile environment, t wireless sensors works unattended and the nodes are highly transitive to capture. that the key are associations with the network clusters and the group keys provide more methods for maintaining session keys [10].

Table 1. Key management functions in static and dynamic keying.

(Admin. Keys Assumed)	Static Keying	Dynamic Keying
Key assignment	Once at pre-deployment	Multiple times
Key generation	Once at pre-deployment	Multiple times
Key distribution	All keys are pre-distributed to nodes prior to deployment	Subsets of keys are re-distributed to some nodes as needed
Re-keying	Not applicable	Multiple times: requires a small number of messages
Handling node capture	Revealed keys are lost and may be used to attack other nodes	Revealed keys are altered to prevent further attacks

2 | Wireless Sensor Nodes

A wireless sensor is device which contains sensors, processor and communication capability, it contains four main components: the sensors, transceiver, processor and power supply, as shown in *Fig. 1*. The many number of wireless sensor nodes developed, as Mica2 and MicaZ. Wireless sensor developed in a group such as wireless sensor network [11]. They are made up of sensor nodes that may acquire, process and transfer the data over a wireless channel. It is based on the environment what they will use but wireless sensors are classified as terrestrial [12]. Comparing to all wireless sensors are using more Zig Bee technology because it is low cost and power consumption. Bluetooth and wireless LAN/WIFI also will be used in some systems [13]. They are some applicable standard are the IEEE 802.15.3, 802.15.4, 802.11, IEEE 1451.

2.1 | Wireless Sensors in the Home

There are many areas where wireless sensors can applied in home. They are more used in home for security purposes [14]. Other these there are lot of applications such as temperature, lights and fans etc. Wireless sensor network are used in the Robo-Maid Home to enable complete the complex task by the robots with minimal equipment [15]. The service of robot connected to home server in *Fig. 1*. There are various applicants of wireless systems available, the ZigBee was most popular because it is low cost and consumes low power, there is tendency to custom-built the hardware [16].

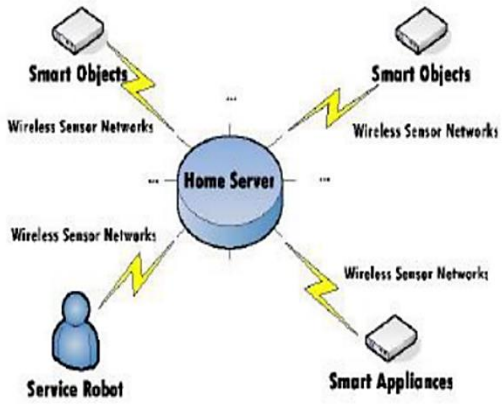

Fig. 1. Schematic diagram of the RoboMaidHome.

3 | Services Provided by Domestic Sensors

Wireless Sensors are useful to home applicants because they will provide lot of services to increase safety and security [17]. There are many applications of wireless sensors in the home: home automation, home

ecurity, energy monitoring, management and conservation, health monitoring and tracking, remote controller, gas detection [18].

Advantage: wireless sensors can detect the presence or absence of people by using this information the system will react, the sensors can detect the abnormal condition of the house holder, and the sensors also can track household gadgets, if they miss anything it will detect the location of the devices [19]. By using wireless sensors if no one is in the room for some time the lights and fans turn off it reduces the consume of energy, wireless sensors are also used to detect the gases.

Disadvantage: in wireless sensors here we see power constraints we will use battery and other portable things. it will do not last long ,we all see our houses need most privacy [20]. We need security in our life here wireless sensor nodes we will be sufficient firewalls, keys, password they should be placed in security intelligence could be incorporated. the cost of wireless sensor network nodes are relatively high [21].

Network architecture: in flat network all nodes are easily identified there will be no predetermined architecture. it will be small and simple network size. It contains lack of scalability. In the multi-tiered architecture it contains scalability; it does not require any table energy and security benefits [22]. Here it reduces the redundancy in the collected data, the flat network nodes will receive high significant traffic volume comparing to remote nodes. The compromise of the cluster does not effect the remaining networks [23].

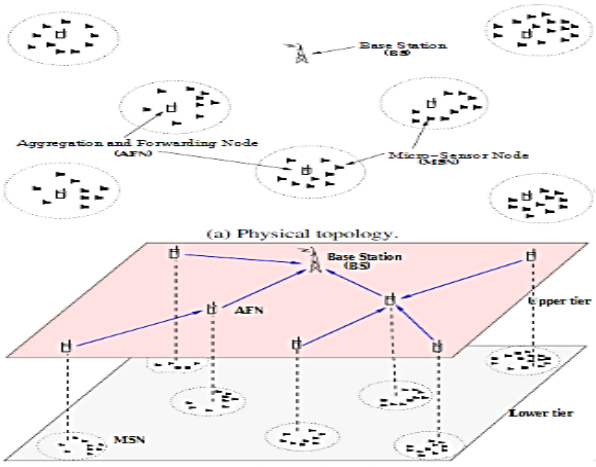

Fig. 2. A two-tiered wireless sensor network.

Fundamental design principles of seck: the fundamental design contains many number of principles in SECK to describe a basic stripped down instance, we will more focus on the way SECK managers key in a cluster.

Threat model: we see that some state nodes have been captured, here we see less server attacks. The least degree of damage it will simply capture nodes at random throughout the network. Here the threats are not addressed in group key. The keys are to be truly effective in a hostile environment. The AFN will not capture immediately. The data which is collected by MSNs in the cluster will be compromised. We need few steps to restore simple operations of the cluster: 1) notify MSNs of the capture, 2) establish a new AFN for each MSN, and 3) establish a new security relationship between the MSN and the AFN.

4 | Evaluation of the Administrative Key Recovery Procedure

The SECK develop d tree administrative keys for the clusters which contains n MSNs where every MSN is having h hope of its primary AFN, *Fig. 3* shows the SECK. The complete administrative key are compression, here the networks have to run the MSN administrative key. here we are having the worst cases when each of the x ca be captured in separate trees. The leaves $d - x$ trees unaffected, and $(d - x)$. Here h nodes can be recovered. Here we see the best cases where the attack is completely localized. The all nodes which are within the single tree are captured before the attacker move; this will affect the [x/h] trees, leaving d-[x/h] trees unaffected. If we repeating the approximate d with n/h, the which can be recovered are (n-h.[x/h])/(n-x)~ 1.

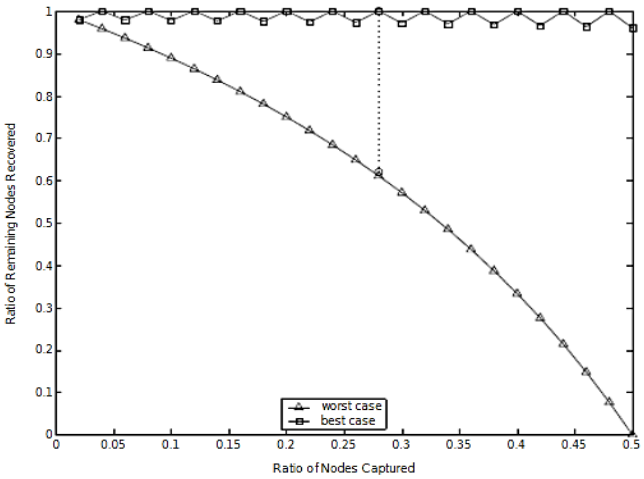

Fig. 3. Graph of administrative key recovery procedure evaluation.

5 | Conclusion

The Domestic applications of wireless sensor network are more used in home and for security purpose. There are many projects regarding which are suitable and helpful. We need the address of the installation and maintenance of wireless sensors, we now a days we are seeing more wireless sensors which are helps in home automation, safety and energy management. In large Scale of WSN clustered formation of sensor nodes and the key management should manage large number of systems. here we have described on cluster-based dynamic keys schema.

References

[1] Mohapatra, H., & Rath, A. K. (2020). Fault-tolerant mechanism for wireless sensor network. *IET wireless sensor systems*, *10*(1), 23-30.

[2] Mohapatra, H., & Rath, A. K. (2019). Fault tolerance in WSN through PE-LEACH protocol. *IET wireless sensor systems*, *9*(6), 358-365.

[3] Mohapatra, H., & Rath, A. K. (2019). Detection and avoidance of water loss through municipality taps in India by using smart taps and ICT. *IET wireless sensor systems*, *9*(6), 447-457.

[4] Mohapatra, H., & Rath, A. K. (2020). Survey on fault tolerance-based clustering evolution in WSN. *IET networks*, *9*(4), 145-155.

[5] Mohapatra, H., & Rath, A. K. (2021). Fault tolerance in WSN through uniform load distribution function. *International journal of sensors wireless communications and control*, *11*(4), 385-394.

[6] Mohapatra, H., & Rath, A. K. (2020, October). Nub less sensor based smart water tap for preventing water loss at public stand posts. *2020 IEEE microwave theory and techniques in wireless communications (MTTW)* (Vol. 1, pp. 145-150). IEEE.

[7] Mohapatra, H., & Rath, A. K. (2022). IoE based framework for smart agriculture. *Journal of ambient intelligence and humanized computing*, *13*(1), 407-424.

[8] Mohapatra, H., & Rath, A. K. (2021). A fault tolerant routing scheme for advanced metering infrastructure: an approach towards smart grid. *Cluster computing*, *24*(3), 2193-2211.

[9] Mohapatra, H., & Rath, A. K. (2021). An IoT based efficient multi-objective real-time smart parking system. *International journal of sensor networks*, *37*(4), 219-232.

[10] Mohapatra, H., & Rath, A. K. (2019). Fault tolerance through energy balanced cluster formation (EBCF) in WSN. In *Smart innovations in communication and computational sciences* (pp. 313-321). Springer, Singapore.

[11] Panda, H., Mohapatra, H., & Rath, A. K. (2020). WSN-based water channelization: an approach of smart water. In *Smart cities—opportunities and challenges* (pp. 157-166). Springer, Singapore.

[12] Mohapatra, Hitesh; Rath, Amiya Kumar: 'IoT-based smart water' [Control, Robotics & Sensors, 2020], 'IoT Technologies in Smart Cities: From sensors to big data, security and trust', Chap. 3, pp. 63-82, DOI: 0.1049/PBCE128E_ch3, IET Digital Library.

[13] Mohapatra, H. (2021, September). Socio-technical challenges in the implementation of smart city. *2021 international conference on innovation and intelligence for informatics, computing, and technologies (3ICT)* (pp. 57-62). IEEE.

[14] Mohapatra, H. (2020). Offline drone instrumentalized ambulance for emergency situations. *IAES international journal of robotics and automation*, *9*(4), 251-255.

[15] Mohapatra, H., & Rath, A. K. (2020). *Fundamentals of software engineering: designed to provide an insight into the software engineering concepts*. BPB Publications.

[16] Mohapatra, H. (2021). *Designing of fault tolerant models for wireless sensor network* (Doctoral dissertation, Ph. D Dissertation, Veer Surendra Sai University of Technology). Retrieved from http://hdl.handle.net/10603/333160

[17] Mohapatra, H., & Rath, A. K. (2020). Social distancing alarming through proximity sensors for COVID-19. *Easy chair*, *18*. https://wvvw.easychair.org/publications/preprint_download/dMGk

[18] Mohapatra. H. (2021). Smart city with wireless sensor network, ISBN-13: 979-8791261380, KDP, 2021.

[19] Mohapatra, H. (2018). *C Programming: practice.cpp*. Independently Publisher.

[20] Mohapatra, Hitesh; Rath, Amiya Kumar, 'Smart Bike Wheel Lock for Public Parking', Application Number: 336834-001.

[21] Mohapatra, H., & Rath, A. K. (2020). Advancing generation Z employability through new forms of learning: quality assurance and recognition of alternative credentials. DOI: 10.13140/RG.2.2.33463.06560

[22] Mohapatra, H. (2009). *HCR using neural network* (PhD's Desertion, Biju Patnaik University of Technology). Retrieved from https://www.academia.edu/29846341/HCR_English_using_Neural_Network

[23] Mohapatra, H. (2019). *Ground level survey on sambalpur in the perspective of smart water* (No. 1918). Retrieved from https://easychair.org/publications/preprint/CWpb