ISSN No:-2456-2165

Review of Wireless Sensor Networks: Challenges and Threats

Ahmed R. Al-Breiki1, HothefaS. Jassim2, Baraa T. Sharef3and Zeyad T. Sharef4

Network and system administration specialist, Information TechnologyAuthority (ITA), Oman1

Modern College of Business & Science Al-Khuwair | 133, Muscat, Oman2

College of Information Technology, Ahlia University, Manama, Bahrain3

College of Engineering, Ahlia University, Manama, Bahrain4

Abstract:-Depending on global telecommunications networks and applying the concept of Internet of Things (IOT) in several applications led to make the need of wireless sensor networks (WSNs) higher than beforein order toachieve a set of basic requirements such as connectivity with networks without human intervention. However, many challenges have appeared and madeWSNs to be targeted by many groups and institutions due toseveral advantageslike using such networks for personal needs or to exploitthem in terms of collecting data for analysis. Nowadays, the security issues for WSN are one of the major challenges which acquire different types of security threats that may cause or appear during the deployment of wireless sensors infrastructure. In addition to that, the restrictions in the process of energy consumption impose a big challenge because of the slow progress in battery technology.Based on several detailed research papers and resources from different aspects that are related to this issue,this paper discusses the challenges which include differentkinds of attacks in WSNs, degree of reliability, energy and susceptibility for programming.

Keywords:- WSN, IOT, Sensors, Challenges, Threats, Attacks.

I. INTRODUCTION

Undeniably, technology is considered as the vain of life. Recently, there is a huge explosion of technology development and revolution. Many devices have been invented to facilitate the human being's life. One of these crucial technologies is wireless sensor networks. WSNscreate a scientific revolution in the field of wireless communications, which make global manufacturing companies ofthese devices that tend to rely on making a small hardware volume with capabilities of wireless connection. Also, they can be easily installed in the devices. WSNs have been distributed and gaining popular in every fields like military, environment monitoring, healthcare and traffic management.[1] TheWSNs can directly interact with the surrounding environment through sensors, which can recognize the physical phenomena such as high temperature, humidity and air pressure. They additionally have a role to measure heart rate and levels of stress for patients.Accordingly, the scientists candeploythe sensors capabilities, link the sensors to wireless networks and carry out the anticipated effectiveness of the tasks. Moreover, after the installation of wireless sensor networks, sensor node will take the role of self-organizing suitable network infrastructure, processing data and routing in wireless sensor networks between sensor nodes. [2]Most of the sensor nods distribute in hostel filed with active intelligent opposition.[3] Because of the limitation of the capacity, memory and power consuming, transferring the data throw wireless sensor networksbecome challenge. [1]Furthermore, the sensor node processes the data and my cause data manipulation, data fraud and replacement. [1]This study specifically talks about the challenges in different kinds of attacks in WSN, the reliability, susceptibility for programming andthe energy.

II. ATTACKS IN WIRELESS SENSOR NETWORKS

Wireless sensor networks can be attacked or exploitedthrough the weaknesses and their vulnerabilities due to the nature of transferring data between sensors/nods and transmission medium. Wireless sensor networks' attacks have been classified as following:

A. Routing Attack

Routing attack occurs in network layer while routing the package. There are different kinds of routing attacks, they are discussed as follows:

- *Sybil attack*

Assign multi fake-identification for many nods while using them in many alternative paths in the network [3][4][12]. Usually, this kind of attack harm peer-to-peer systems and create vulnerable points on them like vehicular Ad hoc Network(VANET) [4]. Also, Sybil attack can attack geographical routing protocol and location based routing protocol because of using multipath routing. [12]. Fig.1 shows the Sybil attack where one of the malware node IDused to connect to their neighbour[14]. When the node

ISSN No:-2456-2165

responds as result, all malware nodes will respond and that will make the neighbour node to confuse and breakdown the network[14].

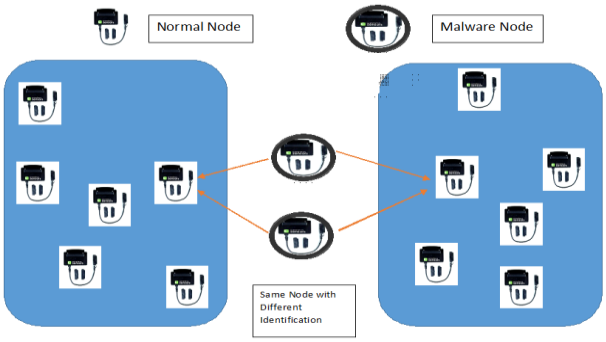

Fig. 1:-Showing how the Sybil/malware node establishes the Sybil attack

- *Black hole attack*

Malware node which pretend to have shortest path in the network by broadcast to the nearby nods to update their routing path to grab all the traffic in the network. [4] while this node is in the network, the packages will not reach to the receiver because all the package are dropped by the malware node. Malware node start working by wetting the nearby(victim) to send RREQ and once it receives this message; will replay with error message RREP for the victim[4]. On that, it will increase the cost number of that rout to be settled in the routing table of victim node before the true node replay with true and genuine message [4] [6].Fig.2shows the malware node when it attracts all the traffics from its neighbor and drop all the traffic of them. [15]

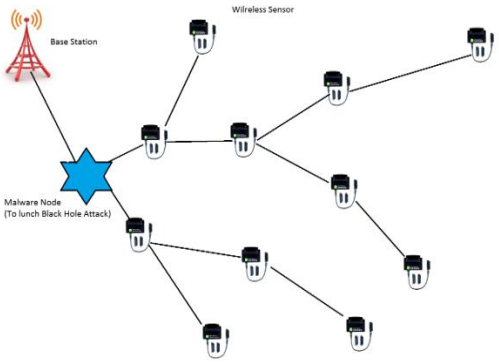

Fig. 2:- Black Hole attack

- *Sinkhole*

The mechanism of this attack is by putting attractive node inside a network to be more popular to the nodes. [3] This kind of attack occurs inside the network after the intruder/hacker compromises a node (malware node) in the network and activates the attack. After the malware node settles down in the network, it will try to reach to the entire neighbor node's traffic to lunches attack on them by exploit the communication way of wireless sensor while sending the data to base station[6].For that reason, the wireless sensor networks become vulnerable to this kind of attack. Fig.3 shows the malware node when it attracts all the traffics from its neighbor by telling them that it the shortest path to the target node[6].

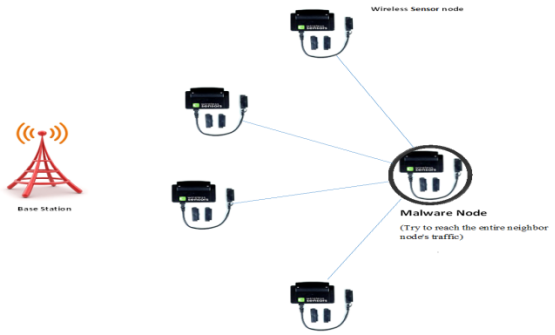

Fig. 3:-A sinkhole attack

B. Denial of Services (DoS) Attack

This kind of attack can be appearing due to failure action of nods or malicious activity and that cause subvert, disrupt and destroy the network. There are different kinds of Dos attack in different layers of OSI protocol and effect in their functionality[3][5]. This attack may happen intwoways, jamming the signal and power exhaustion[11]. For the jamming, it works by sending strong signal to destroy the exchanged message that flow between nodes in the network. The idea ofpower exhaustion is to in destruct the role cycle of sensor/node to loss the battery[11]. Denial of Services path based happen as shown in Fig. 4.

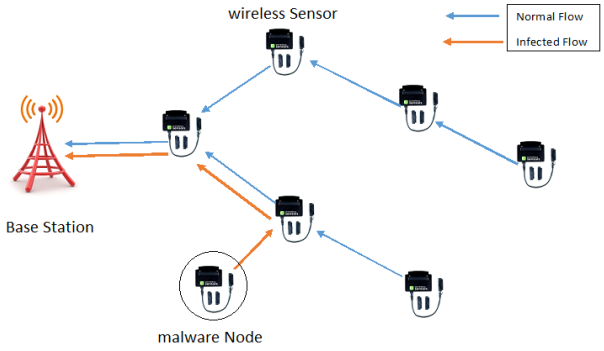

Fig.4:- Path-based DoS attack

C. Hello Flood Attack

In normal situation of the network, every node once itattaches to a network will broadcast hello message to announce themselves to nodes inside the network[7]. For the neighbour node of that nodes, will assume that node is within rang. However, some times that assumption is false because some hackers (malware node) broadcast that message with large power which can be enough to convince all neighbour nodes that the malwarenode is a neighbour for them[4][7].

ISSN No:-2456-2165

D. Wormholes Attack

This is one of the severe kinds of attack that targeting this kind of network. This attack starts by create high-speed channel between two or mode nodes called wormhole link [8]. Fig. 5 shows wormhole link [8] [22].In this attack, the twoends of the wormhole link forms channel to send package and replay that package inside the network [7][8].By that, the attacker/malware node will increase their position in the network [8]. That can be represent in Fig.5. This kind of attack can effect in routing protocol like AODV, DSDV and DSR [7][8].The effect can be representing while the malware node tunnel (using wormhole link) every RREQ message to another malware node which is very close to the destination node of that request [7]. The neighbours dynamically will rebroadcast this RREQ once they hear the request and will ignore other RREQ message that they received [7]. Additional to effecting on routing protocol, this attack can change the topology of the network. Also, the malware node can change message streaming, district and alter the packages.

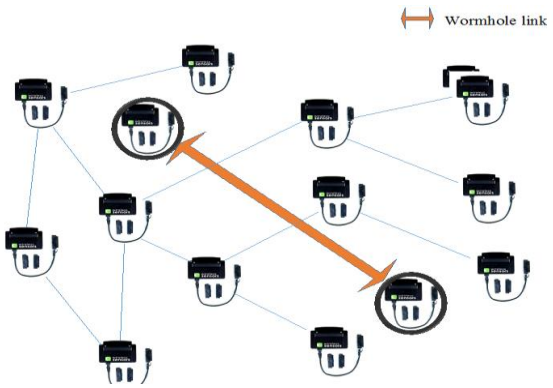

Fig. 5:- Establishing wormhole link between malware nodes.

III. CHALLENGES OF WIRELESS SENSOR NETWORKS

Several kinds of challenges thatinterrupt or affect the performance of a wireless sensor network are presented as follows:

A. Hostile Environment

Deploying and spreading the wireless sensors is the first stage of creating the infrastructure of the wireless sensors networks. On that, they need to take care during the distribution of the sensors to achieve the target requirements. The Hostile nature of the target filed can effect in the way of deploying the sensors. For that, the sensors are vulnerable from different security attacks[13] [18].

B. Power Management

Due to dependency in battery powered, it means the limitation amount of the energy even if there are additional power supplies, so that makes this challenge is very critical[2][9]. For these restrictions, there are expectations to solve this kind of problem but it seems that the restrictions in consuming the power impose big challenges because of the slow progress in battery technology [2] [10].

C. Security and Privacy

The wireless sensors network contrasts traditional networks, sensors are usually deployed in the open and exposed areas of environmental changes, sothe sensors are prone to direct attacks [10].There are many elements that need to be taken into account when dealing with sensor networks including the degree of reliability, security and privacy. For the wireless sensors, usually suffer from transmission error or reception error which can be caused by the collision or traffic in the network. Moreover, the nodes itself prone to failure due to either malfunction or intervention. The nodes of this kind of network interact with surround nodes and people which make other security problems [10]. In addition, securing the wireless communication, Transmission and the environment of the network become more challenges with the different types of attacks [2] [10].

D. Susceptibility to programming

One of the main challenges that is needed to be addressed is the viability of devices in the wireless sensor networks to be programmed. That is given because of the current sensor need from the user to participate in different part of the programming cods where they must prepare and equip communication between sensors and determine assembly ways in addition to other functionalities [10] [22].

E. Real-Time communication

Wireless sensors network interacts with different kinds of real world environments with variants of the natures [10] [20] [21]. The accuracy of the time for delivering packages on real- time is needed to take appropriate observations which can help to take actions on them. There are a small number of result have been find regarding for real-time requirements in wireless sensors network. In case of take the real- time result in account, some of the protocols avoid it and the others try to make to achieve the process before it passes the deadline.Accurate feedback and new results to guarantee real-time are requirements are necessary to be able to deal the realistic of wireless sensors network like lost messages, noise and congestion. That will help to support different routing protocols to enhance and to identify new services that can be used with this wireless network[2] [10] [24].

IV. RECOMMENDATIONS

Nowadays, researchers focus on three different categories to afford security for wireless sensors network; signature management, routing security and authentication, and services to deliver data safely. [17] [23] [24]The Security requirements for the wireless sensors network does

ISSN No:-2456-2165

notaffect the flow of the work only, it's also affect in the availability of the resources in whole the network[17]. It is very important to understand this kind of requirements in order to be able to handle the errors that can happened during the communication [17].The main requirements that are needed to be considered are data integrity, data availability, data confidentiality and data authentication. There are many techniques to insure this kind of requirements like Watermarking technique witch insure the integrity and authenticity of the wireless sensors network. Watermarking is the most popular technique for this purpose which prevents the packets to be intercepted.Fig. 6 shows how this techniqueworks [16]. Intrusion detection system is one the powerful technique that can used in wireless networks which have the ability of differentiating between the activities of the node if it is normal or abnormal in order to define the malware nodes [17]. For preventing from different attaches, there are many techniques and mechanism that can be used in order to prevent many attacks [18][19].For preventing from Denial of Services,message, encryption and authorization mechanism can be used.Also, for wormhole attack, Dawwsen proactive routing protocols can be used which are involved in data link layer of OSI model. Sybil attack candefenseagainst them by using ID certificatesfor the nodes [18].

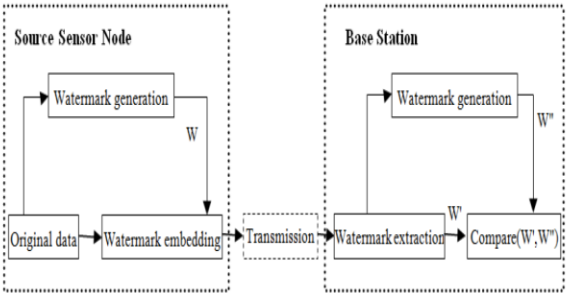

Fig. 6:-Watermarking technique

V. CONCLUSION

In conclusion, every new technology is exposed to different kind of attacks, threats and challenges. Providing the privacy in such wireless sensor networks is a vital need in the network against the attacks.The nature of network deployment area can affect different features of WSNs. Also, power consumption is still considered as a big challenge that has a lot of limitations in performance of the wireless sensors.

REFERENCES

[1] Potins A. and Rajeshwari C. "Wireless Sensor Network: Challenges, Issues and Research" International Conference on Future Computational Technologies (ICFCT'2015), ISBN 978-93-4468-20-0, Issue March 29-30, 2015, pp.224 - 228.

[2] Mahesh P., Kale G. and Jaywant A. "Review: Features, Protocols, Threats and Challenges of WSN".International Journal of Advanced Research in Computer Science and Software Engineering (IJARCSSE2016), ISSN: 2277 128X, Volume 6, Issue 3, March 2016.

[3] Padmavathi G. and Shanmugapriya D. "A Survey of Attacks, Security Mechanisms and

Challenges in Wireless Sensor Networks" International Journal of Computer Science and Information Security (IJCSIS), ISSN 1947-5500, Vol. 4, No. 1 & 2, 2009.

[4] Virmani D., Soni A., Chandel S. and Hemrajani M. "Routing Attacks in Wireless Sensor Networks: A Survey" International Journal of Computer Science and Information Technologies (IJCSIT), ISSN: 0975-9646, Vol. 5 (2), 2014.

[5] Roopak M., bhardwaj T., Soni S. and Batra G. "Review of Threats in Wireless Sensor Networks". International Journal of Computer Science and Information Technologies (IJCSIT), ISSN: 0975-9646. Vol. 5(1), 2014.

[6] Keerthana G., Padmavathi G. "Detecting Sinkhole Attack in Wireless Sensor Network using Enhanced Particle Swarm Optimization Technique". International Journal of Security and Its Applications. Vol. 10, No. 3 (2016), pp.41-54

[7] Virendra Pal Singh V., Jain S. and Singhai J. "Hello Flood Attack and its Countermeasures in Wireless Sensor Networks". International Journal of Computer Science Issues (IJCSI). ISSN: 1694-0784, Vol. 7, Issue 3, No 11, May 2010.

[8] Shree and Khan R. "Wormhole Attack in Wireless Sensor Network". International Journal of Computer Networks and Communications Security (IJCNCS). ISSN: 2308-9830, vol.2, no.1, 2014, pp.22–26.

[9] Gupta A., Rautela B. and Kumar B. "Power Management in Wireless Sensor Networks". International Journal of Advanced Research in Computer Science and Software Engineering. ISSN: 2277-128X, Volume 4, Issue 4, April 2014.

[10] Stankovic J. "Research Challenges for Wireless Sensor Networks".ACM SIGBED Review - Special issue on embedded sensor networks and wireless computing, July 2004,pp. 9-12.

[11] Vidya M and Reshmi S. "Denial of Service Attacks in Wireless Sensor Networks" ISSN: 2319-2526, Volume -3, Issue -2, 2014.

[12] Abirami.K and Santhi.B. "Sybil attack in Wireless Sensor Network". International Journal of Engineering and Technology (IJET). ISSN: 0975-4024, Vol 5 No 2, Apr-May 2013.

[13] Kumar V., Jain A. and Bareal P. "Wireless Sensor Networks: Security Issues, Challenges and Solutions". International Journal of Information & Computation

Technology. ISSN 0974-2239, Volume 4, Number 8 (2014), pp. 859-868

[14] Manjunatha T., Sushma M. andShiva K. "Security Concepts and Sybil Attack Detection in Wireless Sensor Networks". International Journal of Emerging Trends and Technology in Computer Science. ISSN 2278-6856 Volume 2, Issue 2, March – April 2013, pp 383-390.

[15] Baviskar B. and Patil V. "Black Hole Attacks Mitigation and Prevention in Wireless Sensor Network". International Journal of Innovative Research in Advanced Engineering. ISSN: 2349-2163, Volume 1 Issue 4, May 2014, pp 167-169.

[16] Sun X., Su J., Wang B. and liu Q. "Digital Watermarking Method for Data Integrity Protection in Wireless Sensor Networks". International Journal of Security and Its Applications.Vol. 7, No. 4, July2013, pp 407-416.

[17] Ali S. "Intrusion Detection System in Wireless Sensor Networks".International Journal of Science and Research. ISSN: 2319-7064, Volume 4 Issue 7, July 2015, pp 1052-1058.

[18] Sharma K. and Ghose M. "Wireless Sensor Networks: An Overview on its Security Threats". International Journal of Computer ApplicationsSpecial Issue on MANET, 2010, pp 42-45.

[19]SR Al Dhabooni, HS Jassim, ZT Sharef and BT Sharef. "Survey: Security Attacks in Wireless Sensor Networks". International Advanced Research Journal in Science, Engineering and Technology, 2017.

[20] KA Rasbi, H Shaker and ZT Sharef. "Survey on Data-Centric based Routing Protocols for Wireless Sensor Networks". International Journal of Electrical, Electronics and Computers, 2017, pp.9-16.

[21] BT Sharef, RA Alsaqour and M Ismail."Vehicular communication ad hoc routing protocols: A survey".Journal of network and computer applications, 2014, pp. 363-396.

[22] ZT Sharef, AE Alaradi and BT Sharef. "Performance evaluation for WiMAX 802.16e OFDMA physical layer". IEEE Proceedings of Fourth International Conference on Computational Intelligence, Communication systems, and Networks, 2012, pp. 351-355.

[23] B Tariq, R Alsaqour, M Alawi, M Abdelhaq and E Sundararajan. "Robust and trust dynamic mobile gateway selection in heterogeneous vanet-umts network", Vehicular Communications, 2018.

[24] BT Sharef, RA Alsaqour, M Ismail and SM Bilal. "A comparison of various vehicular ad hoc routing protocols based on communication environments". In ACM Proceedings of the 7th International Conference on Ubiquitous Information Management and Communication, 2013, p. 48.