www.mecsj.com

Security Mechanisms and Challenges in Wireless Sensor Networks

Salma ALqahtani

Computer Science department, University of the people

E-mail: researcher.2018@gmail.com

Abstract

With the emerging trends in technology that are aimed at making the world a global village, various moves have been made to bridge communication gaps as well as simplify overly complex tasks. Among those innovations, the introduction of Wireless Sensor Networks has been welcomedfrom all quarters based on the many advantages it brings forth (Perrig, Stankovic & Wagner, 2004). This paper explores Wireless Sensor Networks (WSN) as an emerging technology with an immense capacity to completely transform daily experiences, ranging from risky military environments, traffic control, surveillance to accident detection just to name a few. For the WSNs to achieve their intended goals, it is necessary that security is prioritized to reduce the risk of compromise, looking at the intricate roles the technology plays, for instance, military applications (Gungor, Lu & Hancke, 2010). Furthermore, by considering the nature of WSNs operations, which revolves around detecting very intense threats, false alarms would negate the essence of embracing the WSN oriented systems. In a nutshell, the sensing technology bears many futuristic oriented ideas, if well explored will make life easier for generations to come (Romer & Mattern, 2004). Addressing the current and potential challenges guarantees that this crucial WSN technology is taken as seriously as should. The purpose of this paper is to explicate the security mechanisms and challenges in Wireless Sensor Networks, scoring on the threats as well as proposed solutions for the WSN related drawbacks. This is achieved by embracing a holistic approach as presented herein.

Keywords: Security Mechanisms, emerging technology, Wireless Sensor Networks

www.mecsj.com

1. Introduction

As suggested by the name, the term Wireless Sensor Network represents a network that is made up of a number of sensors incorporated in a given base station. The network is founded on a number of sensor nodes that are set up in a specified sensor field and thus enhance the capture and routing of the desired information back to the aforementioned base station. In recent years, the Wireless Sensor Networks (WSN) have seen to be embraced in many departments, like the military where they are stationed to identify enemy troops, and also the weather focus department, where meteorologists make use of the wireless sensors to detect and compute humidity, temperature among other uses (Perrig, Stankovic & Wagner, 2004). To enhance the communication between the sensors, developers incorporate transceivers that make use of Radio-Frequency (RF) technology to facilitate the in-range connectivity. Despite the numerous advantages the WSN have availed , it has been noted that the technology comes with a number of issues, that researchers have shownimmense dedication to resolve by coming up with counter mechanisms (Karlof & Wagner, 2003). This paper is dedicated on pointing out the challenges that are inhibiting the application of WSN, alongside the mechanisms, both adopted and proposed aimed at resolving the drawbacks.

2. Requirements in Wireless Sensor Networks

By design, the sensors are formulated in a way that they meet certain requirements that enhance security by guaranteeing that security protocols are observed (Ye, Luo, Cheng, Lu, & Zhang, 2002). As a result, the moment a breach as well as compromise of the requirements is witnessed, the impact of the same is tremendous, from giving inaccurate feedback to complete destruction of the set up networks. The requirements revolve around;

A. Data Integrity

www.mecsj.com

Integrity is a major framework behind the adoption and use of the WSN, looking at the intricacy of operations that are carried out using this technology. Data integrity is the guarantee that the sender sends whatever it is exactly what is received by the receiver, inasmuch as there may exist third parties with malicious intent to hijack the data packets transferred. In other words data integrity is all about packet congruence, where what has been conveyed is exactly what is reflected on the other end (Karlof & Wagner, 2003).

B. Confidentiality

Confidentiality narrows down the focus to network and is driven by the tenet of security of the data being conveyed. The unwelcome third party access in question is barred from not only making adjustments but also reading the data that is being transferred. For instance, in state intelligence operations, whereby if the information falls into the wrong hands can create a catastrophe and even jeopardizing critical military operations. By this accord, WSN is set up with secure end to end encryption capacities to minimize the threat of vital data and information compromise (Khan, Shah & Sher, 2011).

C. Authentication

In the WSN context, authentication is used to represent the measures put in place to ensure that the person or device embracing the sensor technology is permitted to do so. Furthermore, authentication tones down to the message itself, making sure that retention of the original properties of the conveyed message regardless of the sophisticated means that may have been used to enhance the communication. This is made possible through the WSN nodes manifesting high encryptions with primary keys and signatures only known to the sender and receiver, that flagship the authentication (Gungor, Lu & Hancke, 2010).

D. Self-Organization

Based on the variety of applications, the WSN models are designed to manage sensor nodes are a city designed to have the capacity to adjust their properties according to the specific

www.mecsj.com

environments (Romer & Mattern, 2004). For instance, in the transport industry, the WNS technology can be tweaked to not only detect accident risks but also, point out the driving under influence (DUI) individuals. The rationality behind this framework guides researchers to develop sensor nodes that can be able to hold together the emergent situations.

E. Data Freshness

Data freshness refers to the initiative to ensure prompt transfer of the intended packets, as they get to the desired situations. Based on the fact that the WSN technology is used in areas where prompt updates area is necessary. for example, looking at the computations in meteorological studies markedly temperature and humidity, the data is fresh to enhance the robustness of the data collected (Khan, Shah & Sher, 2011). Taking a closer look on the issue presents the vulnerability, this data freshness requirement elicits as an attacker can go ahead and tamper with packets to expire creating contention and as a result stale communication, which may stand in the way of effective functionalism.

F. Availability

The availability requirement is developer oriented, and thus explores the ease access to the sensory nodes, when and if required. In instances where nothing much is happening within the designated environment, the nodes can be left to energy save whereas in high tone activities, the nodes should express willingness to carry out the intended functions (Romer & Mattern, 2004).

G. Flexibility

The nature of WSN environments dictates that from time to time changes are made to the sensor devices in place to ensure that they allow the sought network (Karlof, & Wagner, 2003). For instance, the uncertainty of weather conditions, whereby due to the application areas like battlefields the users have no other use but to stick with the WSN, it is only sane that the devices are flexible in order to retain their properties which will ensure they yield the desired results.

H. Secure Localization

www.mecsj.com

The WSN technology is radio frequency bound; meaning that the places the nodes are set up determine the receivership of the desired packets in the base stations (Romer & Mattern, 2004). Researchers have been able to establish over time that in order to identify the most appropriate point to set up the sensor nodes, it is crucial that they establish mechanisms that will allow data forwarding alongside having trust that in the physical location. Also important is the fact that there are two types of localization markedly; range freebased and range based. In the WSN context, developers have adopted the range-based ones, due to the certainty in the areas where the data transfer is expected to take place in.

3. Challenges in Wireless Sensor Networks

In the application of WSN it has dawned on researchers, engineers, and all the concerned stakeholders, that despite the efficiency the technology accords man, there are still a couple of drawbacks that are inhibiting the full adoption of the WSN ideals. This section lays emphasis on the series of attacks on the WSN that cripple operations, focusing on their nature and impact in the wireless sensor networks arena.

A.　　Active attacks

Active attacks are the physical alterations on the setup devices, which may include damages, blockage of data flow just to name a few. Considering the physical alterations caused by this type of attacks, it is easier to identify when the attack has taken place making it easier for the host party to make the necessary adjustments to deal with the potential setbacks arising from the data compromise before the challenges further heighten (Gungor, Lu & Hancke, 2010). Moreover, in this kind of attacks, the attacker seeks to dismantle some functions in the system with the aim of preventing the data packets transfer that the party carrying out the attack considers hazardous for them. In military operations for instance, the moment troop A. realizes that its operations are being tapped by enemy troop B. by the use of WSN technology, they can

www.mecsj.com

opt to use their expertise to hunt and then bring down the enemy sensor nodes mirroring their intelligence back to their enemy's base station (Karlof & Wagner, 2003). This susceptibility of nodes to physical destruction has for a long period of Time-provena challenge for innovators, who are working dedicatedly with the aim of coming up with untraceable nodes by people with malicious intents (Perrig, Stankovic & Wagner, 2004).

B.   Passive attacks

Passive attacks are the type of attacks where the attacker is careful not to cause physical alterations as they may evoke detection. The rationality is simple, employ patience and learn the weak links in the WSN system and then wait to attack when and if appropriate to do so. In a nutshell, the fact that the passive attacks take time and planning their impact is weighty as the attakers seek to attack the intricate areas (Culpepper & Tseng, 2004). Furthermore, the passive attackers that revolve around information sabotage and back channeling sometimes pave way for the active attacks, as the attacker identifies the hubs along which specified WSN operations revolve. This means that by attacking, the attacker has a better chance of causing bigger damages, which may take a long time to resolve and worst of all retain anonymity in the whole experience (Gungor, Lu & Hancke, 2010). This is to say, in the passive attack frameworks, a system can be attacked and completely brought to its knees, but then it becomes a big issue to establish who triggered the mishap. As a result, the system can be completely vulnerable as the attacker could have accorded themselves with loophole capacity for future attacks (Ye, Luo, Cheng, Lu, & Zhang, 2002).

C.   Flood Attacks

According to Karlof and Wagner (2003) flood attacks can be defined as a distributive denial of service threats that are intended to compromise the authenticity of a given data or information. The concept of flood attacks was induced in wireless sensor networks in 2003, which have been a major challenge to operationalization as the series of commands prompted on the setup

www.mecsj.com

networks can be overwhelming. The attacker auto sends an automated flood of Hello messages that trick the system into adopting the new network as an ally and even begin sending data packets blindly without knowing that the new network that has been introduced into the connection media is that of an attacker with ill motives. Furthermore as the attacker would have analyzed the system and detected the weaknesses linking new nodes in what the paper had earlier on aforementioned as localization creates the illusion that the new node is interlinked and thus not dangerous, which is not normally the case. Subsequent surprise attacks on the exposed WSN cripple down the system, from all corners leading to the collapse of the system as the host cannot pinpoint the exact node ,which by now would have replicated the properties of the others, that is behind the attack (Culpepper & Tseng, 2004).

D.   Black hole attack

According to Culpepper and Tseng (2004), black hole attacks can be identified as the type of attacks in which the attacker designates nodes that comes across as black holes meaning that the nodes can be able to derive information that is transmitted over host network through retrieval of data packets. Additionally, by using the information collected, the attacker node can create a fake data and information aimed at steering the host into a sink hole. It is critical to note that upon the creation of these vulnerabilities, any node is transmitting data to the host base station, also replicates the exact same packet data to the attacker stations (Zhang, Cheng, Shi & Chen, 2016). Armed with the packets the attacker is set in a better position to extract the desired information in relation to the needs of him. Notably, the attacker can choose two methods to disempower the host completely whereby; one, the packets recovered can routinely be dropped to host on the already compromised network, and two, the attacker can opt to selectively embrace a greyhound attack sequence, dropping n attacks at t seconds. This is made possible using the shortest possible paths (Ye, Luo, Cheng, Lu, & Zhang, 2002).

E.   Denial of Service Attacks

www.mecsj.com

This type of attack was made prominent by Gregg, Blackert, Heinbuch & Furnanage (2001) who defined the essence of the DoS attack as to facilitate the wastage of time and resources in the target attack network. The concept of this type of attack is distinguishable as the attacker with malicious intentions uses nodes to convey extra packets with no need at all besides flocking the base station with traffic. This in turn, makes it difficult for the authentic users to be able to send and receive data and information over the affected network (Perrig, Stankovic & Wagner, 2004). Therefore, it is correct to hold that the intent of the DoS attack is to inhibit smooth utilization of the WSN enabled networks, by declining the host and validated users the opportunity to conduct their intended tasks. Significantly, also, the DoS attacks assume variance from layer to layer in the Open System Interconnection (OSI) model. For instance, it appears in form of delays and sometimes is manifested through collision of frames in data link layers and irregular data in the network (Zhang, Cheng, Shi & Chen, 2016).

F.   Sybil Attack

This attack is characterized by the node changing the IDs which heightens resource utilization while in so doing discrediting data integrity. Moreover, the attacker uses the above identified multiple IDs to request authentication and permission which creates suspicion that slows down connectivity, as the Sybil attack center scores on data aggregation. Due to the vicious nature in which Sybil attacks cripple WSN applications in the recent years, researchers have shown efforts to identify the challenge areas with significant counter steps made in the right direction. Khan, Shah & Sher (2011) argue that the attacks can be controlled, especially in WSN where the base station acts as the command hub eliminating false node requests for permission. Additionally, Raspotnik (1998) opine that Radio Frequency (RF) technology can be used to detect Sybil attacks, eliciting the use of countermeasures.

4. Security Mechanisms

www.mecsj.com

Looking at the security threats mentioned above as well as the rest that keeps cropping every single day, developers and researchers in the Wireless Sensor Network spectrum have come up with mechanisms over the years that seek to address the threats. This section identifies the prevention mechanisms as discussed herein.

A.   Denial of Service Attack

Denial of service attacks aims to jeopardize the operationalization of the network, whereby more resources than necessary are requested, that causes jamming of the networks. Over time, WSN strategy have established that the first step towards resolving the jamming contention is to identify jammed segment of the sensor network, allowing correction of the unavailable portion (Culpepper & Tseng, 2004). The nodes are set up in such a way that incase of any jamming, they can auto detect the discrepancy and transmit the reports to the neighbor nodes. As a result, the node regions along the network can collectively pinpoint the affected region hence creating the necessary physical insulation to counter further DoS attacks (Zhang, Cheng, Shi & Chen, 2016).

B.   Sybil Attack Remedy

The Sybil attacks as identified triumphs with multiple ID creation which in turn slows down the authentication hence triggering lagging in WSN applications. In order to counter the Sybil challenge, the system should be configured in such a way that the session primary key keeps changing in that set time. Taking these measures invalidates the commands sent by the attacker nodes, as it would prompt them to enter the primary key they do not have. Moreover, by physically enabling protection on the networks, the attacks can be identified and resolved before they yield serious consequences (Khan, Shah & Sher, 2011).

C.   Spoofing and traffic analysis

Spoofing in the Wireless Sensor Network can be defined as the tendency of an attacker to masquerade or falsify data while aiming to have an illegitimate advantage that mainly revolves around back channeling with malicious intent (Yang, Chen, Trappe & Cheng, 2013). This

www.mecsj.com

practice is vicious in the WSN context as it elicits loopholes for regular attacks like the ones discussed in this paper. Armed with this knowledge, it has become important to seek understanding of the spoofing and traffic ideals to be better positioned to counter spoof related drawbacks (Gungor, Lu & Hancke, 2010). By monitoring all the sensory nodes, and also conveying dummy packets instead of the real ones, the host is able to derail the attacker. Furthermore, the system can be set up in such a way that whenever multiple incorrect entries are made, the system denies permission.

D.   Detection of Node Replication and Intrusion Detection

According to Venkataraman (2007) node replication can be identified and inhibited if two procedures are followed. The former makes use of line multicast and the latter, randomized multicast. The former creates unique keys and protected paths that inhibit duplication, meaning that the moment an attacker replicates a given node and attempts to trick the base hub into packets sending, the administrator managing the WSN is notified and can take the appropriate measures. Conversely, the latter randomly acts to identify inconsistencies in replicated data and raise the intended alarms. Shifting gears to the intrusion detection aspect, the emphasis is put on behavior. This is to say, an intruder node has the tendency to demonstrate abnormal and discrepant behavior that does not sync with normal nodes. Identifying the illegitimacy facilitates identification and aversion of malicious intents.

Conclusion

Wireless Sensor Network is future-oriented technology that is commendable looking at the shortcomings the tech+nology is laser-focused on overcoming. WSN acts as the bridge between current and future human lifestyles; due to the efficiency it elicits (Romer & Mattern, 2004). However, the technology has been inhibited by limitations, most of them stemming from security hitch backs. As illustrated in this paper, various mechanisms have been adopted to address the

www.mecsj.com

issue, most of them are being encryption and cryptography motivated (Gungor, Lu & Hancke, 2010). With the advent rise of data insecurity cases, innovators should seek to look beyond these measures to guarantee attainment of the infinite potential WSN accord.

References

- Culpepper, B. J., & Tseng, H. C. (2004, October). Sinkhole intrusion indicators in DSR MANETs. In *Broadband Networks, 2004. BroadNets 2004. Proceedings. First International Conference on* (pp. 681-688). IEEE.

- Gregg, D. M., Blackert, W. J., Heinbuch, D. V., & Furnanage, D. (2001). Assessing and quantifying denial of service attacks. In *Military Communications Conference, 2001. MILCOM 2001. Communications for Network-Centric Operations: Creating the Information Force. IEEE* (Vol. 1, pp. 76-80). IEEE.

- Gungor, V. C., Lu, B., & Hancke, G. P. (2010). Opportunities and challenges of wireless sensor networks in smart grid. *IEEE transactions on industrial electronics*, *57*(10), 3557-3564.

- Karlof, C., & Wagner, D. (2003). Secure routing in wireless sensor networks: Attacks and countermeasures. *Ad hoc networks*, *1*(2-3), 293-315.

- Khan, M. A., Shah, G. A., & Sher, M. (2011). Challenges for security in wireless sensor networks (WSNs). *World Academy of Science, Engineering and Technology*, *80*.

- Perrig, A., Stankovic, J., & Wagner, D. (2004). Security in wireless sensor networks. *Communications of the ACM*, *47*(6), 53-57.

- Raspotnik, W. B. (1998). *U.S. Patent No. 5,832,090*. Washington, DC: U.S. Patent and Trademark Office.

- Romer, K., & Mattern, F. (2004). The design space of wireless sensor networks. *IEEE wireless communications*, *11*(6), 54-61.

www.mecsj.com

- Venkataraman, H. (2007). *Performance analysis of multihop ad hoc and hybrid wireless networks* (Doctoral dissertation, Jacobs University Bremen).

- Yang, J., Chen, Y., Trappe, W., & Cheng, J. (2013). Detection and localization of multiple spoofing attackers in wireless networks. *IEEE Transactions on Parallel and Distributed systems*, *24*(1), 44-58.

- Ye, F., Luo, H., Cheng, J., Lu, S., & Zhang, L. (2002, September). A two-tier data dissemination model for large-scale wireless sensor networks. In *Proceedings of the 8th annual international conference on Mobile computing and networking* (pp. 148-159). ACM.

- Zhang, H., Cheng, P., Shi, L., & Chen, J. (2016). Optimal DoS attack scheduling in wireless networked control system. *IEEE Transactions on Control Systems Technology*, *24*(3), 843-852.