SCITECH
RESEARCH ORGANISATION

Volume 10, Issue 2
February 7, 2018

Journal of Research in Business, Economics and Management
www.scitecresearch.com

Wireless Sensor Network Security: Approaches to Detecting and Avoiding Wormhole Attacks

Derek Mohammed[1], Marwan Omar[2], Van Nguyen[3]
[1,2,3]Saint Leo University, School of Business, Florida, 33544

Abstract

This paper explores Wireless Sensor Networks (WSNs) and the related security issues and complications arising from a specific type of security breach, the wormhole attack. Wormhole attacks against WSNs are classified as passive, external laptop-class threats. Because malicious wormhole attacks are increasing, these attacks pose a serious security threat and increase the costs to maintain a Wireless Sensor Network. Research into preventing wormhole attacks yields two distinct model approach types: Administrator-Viewpoint models and User-Viewpoint models. While the modalities vary, the four Administrator-Viewpoint models reviewed were designed in the early 2000s and suggest defending against wormhole attacks through the use of expensive hardware, packet leashes, or topology visualization systems. On the other hand, the four proposed User-Viewpoint models have become the current theoretical models of choice. While existing as simulation approaches to defend against wormhole attacks, the User-Viewpoint models use internally calculated routing algorithms to suggest routes to avoid or evade, not defend against, established wormhole routes. This paper confirms the efficacies of the User-Viewpoint models in the lab simulations are viewed as the most promising cost-effective, future security solutions to wormhole attacks.

Keywords: Wireless Sensor Networks; Wormholes; Security; Sensor Nodes.

1. Introduction

Wireless Sensor Networks (WSNs) are autonomous, spatially distributed nodes which function in hostile or remote environments to monitor physical or environmental conditions. These nodes work cooperatively to identify and solve problems through nodal localization (Honglong, Wei, Xice, & Zhi, 2010). For the most part, these wireless sensor networks forego any fixed infrastructure in favor of an ad-hoc topology utilizing various types of unattended wireless communication channels (Sharma and Bhadana, 2010). WSNs were originally devised to handle military applications, perform border surveillance, or monitor battlefield conditions (Mahadevi, 2011). In response to the successful military outcomes achieved, in recent years, civilian applications such as healthcare and environmental monitoring, traffic control, and home security automation have abounded (Meghdadi, Ozdemir, & Guler, 2011).

With each new advancement in integrated circuit and sensor technology, wireless sensing devices have become less expensive, but, at the same time, these devices have increased in overall capabilities and, surprisingly, in the security risks posed to users (Jagadeesan, 2016). While WSNs are vulnerable to a wide variety of security attacks, this paper gives an overview of the components of WSNs, defines key terms, addresses the threats posed to wireless sensor networks by wormhole attacks, and suggests potential or proposed security schemes to forestall wormhole attacks and the resulting damage to network hardware, systems, and data.

2. Wireless Sensor Networks

Wireless Sensor Networks differ from traditional wireless networks. WSNs consist of a hierarchical, three-layered architecture and three sensor node types. WSNs are a form of distributed information aggregation system. Unlike traditional wireless networks, WSNs are limited in energy, communication capabilities, memory, and computational

abilities. As a result, a WSN's reliability and precision are considered to be less reliable and precise than a traditional wireless network. At the heart of a WSN are three types of densely deployed nodes for collaboratively sensing, processing data, and communicating information and results. The three types of nodes are sensor nodes (SN), forwarding nodes (FN), and access points (AP). These nodes have the capability to freely roam within a widely dispersed network. Individual nodes essentially transmit data and serve as information routers for other nodes (Qiu, Zhou, Baek, & Lopez, 2010).

According to Sharma and Bhadana (2010), sensor nodes are low power, have limited functionality, and are not individually capable of multi-hop routing. These nodes tend to be application specific to monitor temperature, video, or pressure. Most often, sensor nodes are grouped in clusters and sited at strategic locations. Sensor nodes monitor applications or provide surveillance to send back to the local forwarding nodes (FN). For each sensor node cluster, there is an individual forwarding node (FN). Forwarding nodes receive the sensor node cluster information and then process the information to obtain aggregate results. These nodes also verify the information received from the SN cluster. This "middle man" node consists of two wireless interfaces between the lower level sensor nodes and the next higher level of node, the access points (AP). Possessing both wired and wireless interfaces, access points (AP) utilize its multi-hop routing capabilities to send SN and FN packets to wired networks within a designated radio range as well as to forward control information between SNs and FNs and wired networks. APs also are capable of re-verifying the information previously verified at the FN node level.

At each of these node points, protected and authenticated communication between the various sensor nodes are key security concerns. WSN sensor node vulnerabilities arise from four separate areas: the open nature of wireless channels, the absence of infrastructure, its rapid speed of deployment, and hostile deployment environments (Tun and Maw, 2008). Due to these four vulnerabilities, security protocols centered solely around physical security cannot be successfully used. Security only becomes more critical against security attacks because sensor nodes are heavily constrained and limited in terms of its internal energy, memory, computational and communication abilities. Because it's routing paths and relative neighborhood are subject to constant change, networks frequently cannot provide adequate security measures against posed threats such as breaches in confidentiality, integrity, authentication, and authorization (Bankovic, Fraga, Moya, & Vallejo, 2012). There is little or no capability to identify new threats or impending attacks and to react proactively to prevent damage. Security, then, becomes a paramount concern because roaming nodes have to constantly be authenticated within neighboring nodes through secure communication keys.

Attacks on WSNs can be categorized as passive or active and internally-sourced versus externally-sourced attacks. More specifically, there are two view levels of attacks: security mechanism attacks and basic mechanism attacks. Major attacks can consist of wormhole attacks, spoofing, selective forwarding, black-holes or sinkholes, Sybil attacks, HELLO flooding, and denial of service Of these attack sources, wormhole attacks, the focus of this paper, constitute one of the highest continuing threats to WSNs (He, Ma, Wang, & Fang, 2009). Wormhole attacks are malicious, passive, external laptop-class threats. In a wormhole attack, at least two colluding nodes maliciously "create a higher-level virtual tunnel (wormhole) in the network and transport message packets between the tunnel endpoints" (Kumar, Waheed, & Basappa, 2010) by offering shorter network links. Unsuspecting nodes are deceived into selecting the shorter routes and replaying the message in a separate part of the network and corrupting data or disabling networks through faulty information. Wormhole tunnels can be established through wired infrastructure links or hidden within out-of-band channels, through high powered transmission lines, or through packet encapsulation above network layers.

3. Analysis of Prevention Methods

Generally, research into wormhole attack prevention centered on two approaches: Administrator-Viewpoint models and User-Viewpoint models. Each of these approaches was examined to determine its focus, strengths, and weaknesses. In addition, these approaches constituted a representative sample of the multitude of theories, approaches, and models used to address wormhole attack security issues within the information technology industry.

In the Administrator-Viewpoint models, designers tried to identify actual wormholes and then create systems or processes to defend against the attack. Most often, these involved creating models, signal processing antennas, packet leashes, or topology visualization systems (Shang-Ming, Chi-Sung, & Wen-Chung, 2009). The Administrator-Viewpoint models include the Multi-Dimensional Scaling-Visualization of Wormhole (MDS-VOW) (Wang and Bhargava, 2004), the Graph Theoretical Approach using a Local Broadcast Key (LBK) (Lazos, Poovendran, Meadows, Syverson, & Chang, 2005), the initial TESLA with Instant Key (TIK) protocol model (Hu, Perring, & Johnson, 2003), and later TIK protocol models using Tree Cast architecture (Kumar et al., 2010).

In comparison, the second group of approaches, the User-Viewpoint approaches, utilized routing information and implemented an "avoidance" system whereby at-risk routes were bypassed or evaded. Most often, the techniques

suggested were Hop-count analysis, the Thread Model, and Elliptical Curve Pairing (Rahman and El-Khatib, 2009), and a distance-consistency- approach based secure localization protocol. All of the User-Viewpoint approaches were and remain theoretical, proposed models or laboratory simulations.

The TIK Packet leashes approach utilizes an extended version of the TESLA authentication protocol for instant authentication of broadcast communications and temporal leashes over sensor networks. Packet leashes attempt to span the distances that messages can travel using geographical and temporal leashes. Geographical leashes group certain packet recipients within a defined distance from a sender. Temporal leashes, on the other hand, established a maximum travel distance and set upper lifetime boundaries. Critical to this model was the assumption that all sensor nodes recognized its independent location and then embedded a time and site location stamp within each sent packet. With network synchronization, these special packets easily ferreted out wormholes based on time and location anomalies; however, if synchronization failed, the methodology was not useful (Rani and Kumar, 2017).

MDS-VOW, A type of topology visualization system advanced by Wang and Bhargava (2004), employed the use of sensor network nodes within a network's topology to detect wormholes through multidimensional scaling. Based on signal strength, distances between sensors were estimated and mapped by a central controller. The central controller calculated the overall physical topology based on the distance measurements between sensors. Anomaly-free areas presented as flat while wormholes presented as a string-like structure connecting the network edges. This system was most effective for centralized networks and was hardware intensive.

The Graph Theoretical Approach focused on communication range capabilities and utilized a local broadcast key (LBK). The LBK enabled a secure ad-hoc network via guard and regular nodes. Through localizing broadcast keys' encrypted transmissions, guard nodes accessed data location and broadcast the location to regular nodes. Using the guard beacons, the regular nodes calculated a sensor's location. Any abnormal transmissions arising from wormhole attackers could easily be distinguished and isolated. Time delays were graphed and delay times were calculated using special localization equipment (Lazos et al., 2005). Any delays more than twice the radius between nodes were deemed an anomaly. This system's major weakness was that all guard nodes must be able to know exact locations at all times. It was most suited for a stationary dense sensory network. Seven years after the initial TIK protocols were implemented, Kumar et al. (2010) suggested an updated TIK stateless architecture with disclosed public values and symmetric cryptography called Tree Cast. This stateless architecture was facilitated by the technology advances in low-power and low-cost wireless sensors. Multiple disjointed message trees created geographically intertwined and rooted address allocations in a data sink. The trees routed messages back and forth to the data sink; however, no sensor node routing states were required. Received packet leashes provided instant authentication using only a modest storage size and computational overhead.

In the Hop-count approach (Shang-Ming et al., 2009), the authors formulated a Multipath Hop-count Analysis (MHA), a type of wormhole attack detection scheme which does not require any unique or specialized assumptions about the environment. Instead, it utilized existing routing information established under RFC 3561 to create a multi-path routing protocol which seeks to avoid, not identify, wormholes. The basic premise was that communication pairs normally hold 5-6 hops while wormhole routes have two hops. Avoiding the smaller hop-count routes will result in avoidance of most wormhole attacks through a four stage process: route establishment, gray-list broadcasts, the hop-count analysis scheme, and route maintenance. In this simulation, safe routes were established through processing packets. Routes with too few or too high hop-count levels were deemed risky and flagged or gray-listed. Low hop-count levels inferred the presence of a wormhole. On the other hand, high hop-count levels indicated a risk of transmission deceleration or potential for route breakage. Packets which failed to meet the criteria of a normal route are flagged or gray-listed. Based on this information, the hop-count analysis scheme was derived to establish legal routes authority to transmit data. Finally, route maintenance ensured that broken routes are repaired or deleted and that data packets reach a desired destination via repaired routes or newly re-routed avenues. A Hop-count Analysis Scheme did not require any special environments and operated efficiently with lower overhead costs than traditional Administrator-Viewpoint models.

Another type of wormhole detection approach encompassed detecting and preventing wormhole attacks altogether (He et al., 2009). This simple yet effective method to locate wormholes by using an algorithm to identify known locations of beacon nodes. These nodes take on the role of wormhole or anomaly detectors. At the same time, sensor nodes aid in hop counting or finding the minimum number of hop jumps or transmissions between beacon nodes. Once a standard hop size is calculated via the algorithmic formula, any abnormalities or abnormity would be located via probe and alarm messages and then isolated. The key benefits derived from this algorithm were low calculation costs and reduced localization errors.

Rahman and El-Khatib (2009) postulated that advances in Elliptic Curve Cryptography (ECC) made it feasible to incorporate ECC within wireless sensor networks. Identity-based encryption (IBE) and paired based cryptography enabled a single bit of data to identify users and then exchange keys and encrypt the information. Under this proposed model, nodes were capable of dynamically altering IDs and secret locations. Authenticating shared keys

through low-latency links without preloading nodes' shared keys was a major advantage of the model. Because packet information would prescribe a route, only trusted member-neighbors were accepted, therefore, wormhole attacks would not be permitted. Hence, key space and communication overhead were reduced compared to other communication models.

The Distance-Consistency-Based Secure Localization Scheme theorized that wormhole detection, self-localization, and locator identification were the three foundations for the distance-consistency-based secure localization scheme used for defending against wormhole detection [1]. The purpose of the localization scheme was to calculate the probability and effectiveness of detecting an attack using a three-pronged deployment of sensors, locators, and attacker nodes. Mathematical models then calculated the probabilities of attack detection and finding the V-locator nodes distances. Secure localization outperformed other models and was extremely cost effective since no hardware was required.

4. Results

In 2003, the first serious attempts to address wormhole attacks were initiated. All of these working solutions and research initiatives sought to control the malicious data packets from traveling between nodes. Detecting and correcting WSN security issues arising from wormholes begins with node localization, however, the modalities or approaches vary widely. While identifying exact node locations is not always feasible and is certainly cost prohibitive, suggest that wormhole detection costs are generally proportional to the level of protection provided, therefore, security assessments tend to be short-sighted and fail to address a comprehensive approach to meeting security attacks and denial of the root sources of attacks within an established security framework.

The Administrator-Viewpoint approaches are all currently deployed wormhole defense methodologies. The Packet Leashes Approach, MDS-VOW model, the Graph Theoretical Approach, and Tree Cast are all heavily dependent on significant expenditures for hardware, antennas, specialized localization equipment, and packet leashes, as well as for manpower costs in analyzing the scaling and mapping features of node location. Knowing the location of nodes is key to these models, therefore, a major weakness of these models lies in failure of node synchronization or authentication. All of these early approaches seek to defend against wormhole attacks once a system is threatened or has been attacked, therefore, these models only serve to react to existing problems and have no scheme to avoid the attacks altogether.

The User-Viewpoint approaches all represent theoretical models or simulations designed to avoid wormhole attacks through multi-path routes, hopping, and locator encryption coupled with range localization. The Multipath Hop-count Analysis, the Thread Model, Elliptical Curve Pairing, and Secure Localization Approach represent significant trends in wormhole avoidance techniques. Each of these theoretical models and simulations offers significant cost savings since hardware and special equipment is not needed. Instead, since each of these models relies on mathematical equations and algorithms, the overall calculation cost remains low. The greatest downside to the overall User-Viewpoint models is that these methods have not undergone "real world" testing for practicality and usability.

5. Conclusion

With its spatially distributed nodes used to monitor physical and environmental conditions in hostile or unattended sites, Wireless Sensor Networks represent a major means of sensing, processing, and communicating data results for military and civilian purposes and applications. Because data is being transmitted and shared, basic security issues such as authentication, integrity, confidentiality, and availability arise. While a variety of threats can be mounted against WSNs, wormhole attacks represent one of the major threats to a wireless sensor network's security. Wormhole attacks result from the compromising of two or more sensor nodes. Data is intercepted and re-sent to a malicious user, therefore, addressing the source and type of wormhole attacks is critical and time-sensitive.

This paper delineated between Administrator-Viewpoint and User-Viewpoint models. Realistically, the Administrator-Viewpoint models are tested and have been deployed in industry for at least seven years; however, these solutions come at a high cost in terms of hardware and manpower used. On the other hand, the User-Viewpoint models are more recent, but represent a trend toward more cost-effective solutions that rely on mathematical calculations and algorithms. While each of these offers a solution, currently, there is no one all-inclusive answer to forestalling or preventing security issues within wireless sensor networks.

Wormholes are just one of a plethora of security issues or attacks against a network. Resources within industry are limited, therefore, it is highly likely that wormhole attack solutions will be studied, but it will be studied in an overarching scheme of preventing most kinds of security breaches. The most likely scenario is that a business will find the existing solution which suits its individual needs and is cost-effective.

Research in Wireless Sensor Network security abounds. A promising area of research is combining the two approaches under one umbrella: detection and avoidance of wormholes (Shabana, Fida, Khan, Jan, & Rehman,

2016). In this hybrid approach an outlier detection algorithm is used to identify, locate, and screen outlier nodes. An outlier detection algorithm accomplishes an increased outlier detection rate, an improved accuracy rate, and a higher total transmission energy consumption rate average per node. In addition, symmetric encryption and authentication codes aid in data confidentiality, authentication, and integrity of aggregated data.

References

[1] Bankovic, Z., Fraga, D., Moya, J., & Vallejo, J. C. (2012). Detecting unknown attacks in wireless sensor networks that contain mobile nodes. Sensors, 12(8).

[2] He, R., Ma, G., Wang, C., & Fang, L. (2009). Detecting and locating wormhole attacks in wireless sensor networks using beacon nodes. World Academy of Science, Engineering and Technology, 55.

[3] Honglong, C., Wei, L., Xice, S., & Zhi, W. (2010). A secure localization approach against wormhole attacks using distance consistency. EURASIP Journal on Wireless Communications and Networking, 2010, 1-11.

[4] Hu, Y., Perring, A., & Johnson, D. B. (2003). Packet leashes: A defense against wormhole attacks in wireless networks. Proceedings of 22nd Annual Conference of the IEEE Computer and Communication Societies, 3, pp. 1976-1986.

[5] Jagadeesan, S. (2016). Wireless sensor network security. Proceedings of 3rd International Conference on Recent Innovations in Science, Technology, Management and Environment, 16, pp. 202-209.

[6] Jha, M. K., & Sharma, T. P. (2010). A new approach to secure data aggregation protocol for wireless sensor network. International Journal on Computer Science & Engineering, 1(5), 1539-1543.

[7] Kumar, K., Waheed, M., & Basappa, K. (2010, October). TCPL: A defense against wormhole attacks in wireless sensor networks. Paper presented at AIP Conference Proceedings, Ipswich, United Kingdom.

[8] Lazos, L., Poovendran, R., Meadows, C., Syverson, P., & Chang, L. W. (2005). Preventing wormhole attacks on wireless ad hoc networks: A graph theoretic approach. Proceedings of Wireless Communications and Networking Conference, 2005 IEEE, pp. 1193-1199.

[9] Mahadevi, G. (2011). Location discovery with security in wireless sensor networks. International Journal on Computer Science & Engineering, 3(4), 1528-1533.

[10] Meghdadi, M., Ozdemir, S., & Guler, I. (2011). A survey of wormhole-based attacks and their countermeasures in wireless sensor networks. IETE Technical Review, 28(2), 89-102.

[11] Qiu, Y., Zhou, J., Baek, J., & Lopez, J. (2010). Authentication and key establishment in dynamic wireless sensor networks. Sensors, 10(4), 3718-3731.

[12] Rahman, M., & El-Khatib, K. (2009). Secure anonymous communication for wireless sensor networks based on pairing over elliptic curves. Journal of Interconnection Networks, 10(4), 459-479.

[13] Rani, A. & Kumar, S. (2017). A survey of security in wireless sensor networks. Proceedings of 3rd International Conference on Computational Intelligence & Communication Technology, 8, 256-260.

[14] Shabana, K., Fida, N., Khan, F., Jan, S.R., & Rehman, M. (2016). Security issues and attacks in Wireless Sensor Networks. International Journal of Advanced Research in Computer Science and Electronics Engineering, 5(7), 81-87.

[15] Shang-Ming, J., Chi-Sung, L., & Wen-Chung, K. (2009). A hop-count analysis scheme for avoiding wormhole attacks in MANET. Sensors, 9(6), 5022-5039.

[16] Sharma, P., & Bhadana, P. (2010). An effective approach for providing anonymity in wireless sensor network: Detecting attacks and security measures. International Journal on Computer Science & Engineering, 1(5), 1830-1835.

[17] Tun, Z., & Maw, A. H. (2008). Wormhole attack detection in wireless sensor networks. Proceedings of World Academy of Science Engineering and Technology, 46, pp. 545-550.

[18] Wang, W., & Bhargava, B. (2004). Visualization of wormholes in sensor networks. In Proceedings of the 2004 ACM Workshop on Wireless Security (pp. 51-60). Philadelphia, PA: ACM WiSE'04.