The Wormhole Routing Attack in Wireless Sensor Networks (WSN)

Lukman Sharif* and Munir Ahmed*

Abstract—Secure routing is vital to the acceptance and use of Wireless Sensor Networks (WSN) for many applications. However, providing secure routing in WSNs is a challenging task due to the inherently constrained capabilities of sensor nodes. Although a wide variety of routing protocols have been proposed for WSNs, most do not take security into account as a main goal. Routing attacks can have devastating effects on WSNs and present a major challenge when designing robust security mechanisms for WSNs.

In this paper, we examine some of the most common routing attacks in WSNs. In particular, we focus on the wormhole routing attack in some detail. A variety of countermeasures have been proposed in the literature for such attacks. However, most of these countermeasures suffer from flaws that essentially render them ineffective for use in large scale WSN deployments. Due to the inherent constraints found in WSNs, there is a need for lightweight and robust security mechanisms. The examination of the wormhole routing attack and some of the proposed countermeasures makes it evident that it is extremely difficult to retrofit existing protocols with defenses against routing attacks. It is suggested that one of the ways to approach this rich field of research problems in WSNs could be to carefully design new routing protocols in which attacks such as wormholes can be rendered meaningless.

Keywords—Secure Routing, Routing Attacks, Routing Protocols, Wireless Sensor Networks (WSN), Wormhole Attack

1. INTRODUCTION

Wireless and mobile ad-hoc networks are now considered to be the ultimate frontier in modern communications. The technology allows nodes in a network to communicate directly with each other using wireless transceivers without the need for a fixed infrastructure. This is distinctly different from the mode of operation used in traditional wireless networks, such as wireless LANs in which inter-node communication takes place through base stations [20].

A Wireless Sensor Network (WSN) is a particular type of ad-hoc network. The participating nodes are smart sensors, typically the size of a coin, equipped with advanced sensing functionalities (thermal, pressure, acoustic, etc), a small processor, and a short-range wireless transceiver [20]. The nodes exchange data in order to build a global view of the monitored region Figure 1. This data is typically made accessible to the user through one or more gateway nodes [4].

Manuscript received February 8, 2010; accepted March 31, 2010.
Corresponding Author: Munir Ahmed
* London College of Research, UK (l.sharif@lcrl.org.uk), College of Computer Science and Engineering, Taibah University, Saudi Arabia (mahmed@taibahu.edu.sa)

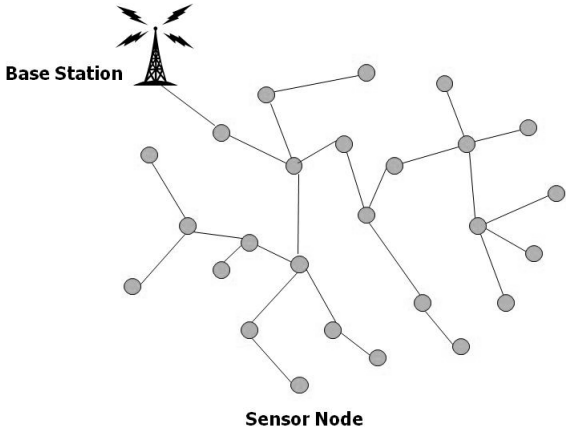

Fig. 1. Sensor nodes exchange data to build a global view of the monitored region

WSNs have tremendous potential to provide very attractive, low cost solutions to a variety of real world problems [4]. The application scenarios for WSNs are many, including military surveillance, commercial, environmental, medical, manufacturing and home automation, to name but a few [1].

The past decade has witnessed an explosive growth in the use of wireless technologies. In particular, WSNs have become a very active area of research [8]. There are many diverse and interesting aspects of this technology which demand further research to produce the innovative solutions needed to make WSNs a viable technology. Routing plays a central role in WSNs. In particular, owing to the inherent characteristics of WSNs, routing security is a hugely important area of research.

In order to maintain the availability of a WSN, resilience to node failure is very important. One of the ways that a WSN node could fail is through an attack [3]. Although many WSN routing protocols have been proposed, none have been designed with security as a main goal [14]. WSNs are vulnerable to a variety of security attacks due to the broadcast nature of the transmission medium [2] and the fact that sensor nodes often operate in hostile environments. Security attacks in WSNs are often classified according the layers of the OSI model. The attacks which operate at the network layer are referred to as routing attacks.

The rest of this paper is organized as follows. Section 2 describes the main characteristics of WSNs which present particular challenges for the design of robust security mechanisms for secure routing. Section 3 outlines the main goals for secure routing in a WSN and presents some of the most common routing attacks in WSNs. Section 4 describes the wormhole routing attack in detail and presents a discussion of some of the countermeasures proposed in the literature for this attack.

2. SECURE ROUTING FOR WSNS: CHALLENGES

Providing secure routing in WSNs is a complicated and challenging task due to the constrained capabilities of sensor node hardware [17] and the properties of their deployment [18]. A brief outline of some of the major constraints present in WSNs is as follows:

2.1 Wireless Medium

The wireless medium is inherently vulnerable due to its broadcast nature [6]. It is relatively easy for an adversary to eavesdrop, intercept, and replay the transmitted data packets and inject malicious ones [6].

2.2 Hostile Environment

WSN nodes are typically deployed in environments where they face the possibility of destruction or physical capture by attackers [2].

2.3 Limited Resources

The extremely limited resources (power, bandwidth, CPU, memory) of sensor nodes are perhaps one of the biggest challenges in the design of robust and often resource-hungry security mechanisms. These constraints necessitate extremely efficient security algorithms [19].

2.4 Ad-Hoc Deployment

The ad-hoc nature of sensor deployment means that the WSN topology is subject to regular changes. Any security mechanisms must be able to operate in such dynamic environments [10].

2.5 Immense Scale

A typical WSN deployment could consist of hundreds of thousands of nodes. Any robust security mechanism needs to be able to scale to such large topologies [6].

3. GOALS FOR SECURE ROUTING IN WSNS

Before we can begin to look at routing attacks in WSNs, it is important to understand what the goals of secure routing in a WSN should be [9].

The role of a routing protocol in any network environment is to ensure that a message reaches a correct receiver in an accurate form and within a reasonable time delay [3]. In an ideally secure WSN routing scenario, we would like to be able to guarantee the confidentiality, integrity, authenticity, and availability of all messages [5] even in the presence of more powerful and resourceful adversaries. For every eligible receiver in a WSN, we would like to be able to receive all messages intended for it and be able to verify the integrity of every message as well as the identity of the sender [7]. Even if an adversary was able to participate in the actual routing, it should not be possible for them to infer the content of any messages [5].

3.1 Routing Attacks in WSNs

Routing attacks have been studied in some detail in [5, 15], and [21]. In general routing attacks are classified as passive attacks and active attacks. In a passive attack, the attacker monitors and listens to the communication channel. Even when the messages transferred are encrypted, it still leaves a high possibility of analysis of the communication patterns. In an active attack, the attacker monitors, listens to and modifies the data stream in the communication channel [11]. Routing attacks are active in nature.

The following routing attacks have been identified in the literature:

3.1.1 Spoofed, altered, or replayed routing information

This type of attack targets the routing information exchanged between nodes [5]. The attacker can spoof, alter, or replay the routing information to create routing loops, generate false error messages and partition the network [2].

3.1.2 Selective forwarding

A malicious node selectively drops and forwards packets to minimize arousing any suspicion among its neighbors [5].

3.1.3 Sinkhole attack

The adversary's goal is to attract all the traffic through a compromised node. Sinkhole attacks try to make routes through a compromised node look especially attractive to surrounding nodes [26].

3.1.4 Sybil attack

A compromised node creates and presents multiple identities to other nodes in the network [15].

3.1.5 Wormhole attack

An attacker records packets at one location in the network and tunnels them to another location, retransmitting them into the WSN [2].

3.1.6 HELLO flood attack

An attacker with a much higher radio transmission range and processing power sends HELLO packets to a number of isolated nodes convincing the nodes that it is their close neighbor. The victim nodes send their packets through the attacker which can then spoof and manipulate the data [2].

4. THE WORMHOLE ATTACK

Wormholes are one of the most severe attacks on WSN routing. Two or more malicious nodes can collaborate in setting up a shortcut lower latency link between each other Figure 2 and through which they forward packets to each other and replay the packets there locally [22].

The adversaries convince the neighbor nodes of these two end points that the two distant points at either end of the tunnel are actually very close to each other [12]. An adversary situated close to a base station may be able to completely disrupt routing by convincing nodes that would normally be multiple hops from a base station that they are only one or two hops away via the wormhole [5]. In such a scenario, the attack is similar to the sinkhole as the adversary at the other side of the tunnel advertises a better route to the base station [1].

Wormhole and sinkhole attacks are particularly difficult to defend against, especially when the two are combined. Wormholes are hard to detect because they use a private, out-of-band

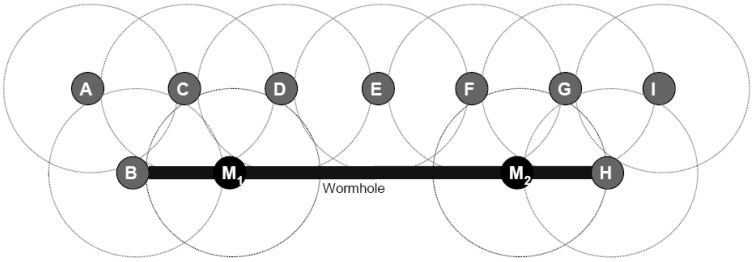

Fig. 2. Two or more malicious nodes collaborate in setting up a shortcut link between each other

channel which is invisible to the WSN [5]. Packets are forwarded between the malicious nodes by encapsulation and use of additional hardware such as a wired link or a directional antenna [16]. Wormhole attacks are more likely be used in combination with selective forwarding or eavesdropping [5]. The wormhole attack is especially difficult to detect in WSNs when using routing protocols in which routes are decided based on advertised information such as minimum hop count to base station [5].

A wormhole attack could be launched in two different modes: hidden-mode and participation mode. Defending against a hidden-mode attack is particularly difficult because it can be launched even if all routing messages are authenticated and encrypted [13]. This is because the malicious node does not need to read or modify the packets, just forward them.

Although participation mode wormhole attacks are more difficult to launch (they require modification of routing packets), once launched, they are extremely difficult to detect since the malicious nodes can simply ignore the security mechanisms of the routing protocol [16].

4.1 Wormhole Attack Countermeasures

A significant amount of research has been carried out into wormhole attacks and a variety of solutions have been proposed.

One particular technique for detecting wormhole attacks requires extremely tight time synchronization between sensor nodes [23] during the route discovery stages. Although this technique has some limited success in small WSNs, it is not particularly feasible for large scale WSN deployments.

One particular class of protocols which seems to be resistant to wormhole attacks is geographic routing protocols [5]. These protocols direct the traffic to the base station along a geographically shortest path and therefore do not rely on advertisements from potential adversaries [24].

A secure routing protocol named SeRWA (Secure Route protocol against Wormhole Attack in sensor networks) has also been proposed [25]. This protocol is able to detect wormhole attacks without needing any special hardware [1].

The vast majority of the proposed solutions for wormhole attacks suffer from flaws such as high cost of implementation and limited scalability. In particular most of these solutions do not address the issue of protection against participation mode wormhole attacks.

A more recent solution [16] is based on the Ad hoc On-Demand Distance Vector (AODV) routing protocol. It proposes modification to AODV to find two or more completely different

routes to the source node. The hop-counts of the found routes are then analyzed to find possible deviant hop-counts. It is assumed that a route with a hop-count value that is significantly lower than others is most likely a wormhole. However, once again, there is no guarantee that this mechanism will work against participation mode wormholes attacks.

5. CONCLUSIONS

Secure routing is crucial to the acceptance and use of sensor networks for many applications. Providing secure routing in WSNs is a complicated and challenging task due to the inherently constrained capabilities of sensor nodes.

Routing attacks can have potentially devastating effects on WSNs and present a major challenge when designing robust security mechanisms for WSNs. Although many different routing protocols have been proposed for WSNs, most do not take security into account as a main goal. We briefly looked at some of the most common routing attacks in WSNs. In particular, we looked at the wormhole attack in some detail. Although a number of different countermeasures have been proposed for this attack, most of these suffer from flaws that essentially render them ineffective for large scale WSN deployments.

Having looked at the wormhole attack and some of the proposed countermeasures, it is evident that it is extremely difficult to retrofit existing protocols with defenses against routing attacks. The inherent constraints found in WSNs necessitate design of lightweight and robust security mechanisms. The task of providing secure routing for WSNs presents a rich field of research problems. Perhaps one solution could be to carefully design new routing protocols in which attacks such as wormholes are rendered meaningless.

REFERENCES

[1] Rehana, J. (2009). Security of wireless sensor network. *Seminar on Internetworking* (TKK T-110.5190). Helsinki University of Technology

[2] Padmavathi, G., & Shanmugapriya, D. (2009). A survey of attacks, security mechanisms and challenges in wireless sensor networks. *International Journal of Computer Science and Information Security (IJCSIS)*: Vol.4, No.1 & 2

[3] Hanapi,. Z.M. Ismail,. M,. Jumari,. K. & Mahdavi,. M. (2009). Dynamic window secured implicit geographic forwarding routing for wireless sensor network. *World Academy of Science, Engineering and Technology*

[4] Deng, H., Li, W., & Agrawal, D. P. (2002). Routing security in wireless ad hoc networks, *IEEE Communications Magazine* (p 70-75)

[5] Karlof, C., & Wagner,. D. (2003). Secure routing in wireless sensor networks: attacks and countermeasures. *Ad Hoc Networks Journal: Special Issue on Sensor Network Applications and Protocols. Vol.1,* (p293-315), Elsevier Publications

[6] Naeem,. T & Loo,. K. K. (2009). Common security issues and challenges in wireless sensor networks and IEEE 802.11 wireless mesh networks. *International Journal of Digital Content Technology and its Applications*: Volume 3, Number 1. (p 89-90)

[7] Lee , J. C., Leung, V. C. M., Wong, K. H., Cao, J., & Chan, H. C. B. (2007). Key management issues in wireless sensor networks: current proposals and future developments. *IEEE Wireless Communications*, (p76-84)

[8] Kavitha, T., & Sridharan, D. (2010). Security vulnerabilities in wireless sensor networks: a survey. *Journal of Information Assurance and Security 5*, (p31-44)

[9] Bojkovic,. Z. S., Bakmaz,. B. M,. & Bakmaz,. M. R. (2008). Security issues in wireless sensor networks. *International Journal of Communications*: Issue 1, Volume 2

[10] Raj,. P. N. & Swadas,. P. B,. (2009). DPRAODV: A dynamic learning system against blackhole attack in AODV based MANET. *International Journal of Computer Science Issues (IJCSI)*: Vol.2

[11] Venkatraman, L., Agrawal, D. P. (2003). Strategies for enhancing routing security in protocols for mobile ad hoc networks. In *Journal for Parallel Distributed Computing.* 63 (p 214-227)

[12] Kalita, H. K., & Kar, A. (2009). Wireless sensor network security analysis. *International Journal of Next-Generation Networks (IJNGN)*

[13] Kaissi, R. E., Kayssi, A., Chehab, A., & Dawy, Z. (2005). DAWWSEN: A defense mechanism against wormhole attacks in wireless sensor networks. *The Second International Conference on Innovations in Information Technology* (IIT'05). American University of Beirut. Beirut, Lebanon.

[14] Karlof, C., & Wagner,. D. (2005). Summary of "secure routing in wireless sensor networks: attacks and countermeasures". In *Seminar on Theoretical Computer Science*

[15] Newsome, J., Shi, E., Song, D., & Perrig, A. (2004). The sybil attack in sensor networks: analysis & defenses. *In Proceedings of Third International Symposium on Information Processing in Sensor Networks.* (p259-268). (ACM 1-58113-846-6)

[16] Jen, S. M., Laih,. C.S., and KuoW,. C. (2009). A hop-count analysis scheme for avoiding wormhole attacks in MANET. In *Sensors*

[17] Kumar, H., Sarma, D., & Kar, K. (2006). Security threats in wireless sensor networks. *IEEE*

[18] Zhou, Y., Fang, Y. & Zhang, Y. (2008). Securing wireless sensor networks: a survey. *IEEE Communications Surveys & Tutorials*. Vol:10, Issue 3, (p 6-28)

[19] Walters, J. P., Liang, Z., Shi, W., & Chaudhary, V. (2006). Wireless sensor network security: a survey. *Security in Distributed, Grid and Pervasive Computing*. (p 3-5, 10-15)

[20] Santi, P. (2005). *Topology control in wireless ad hoc and sensor networks*. Chichester, England: John Wiley & Sons

[21] Hanapi, Z. M., Ismail, M., Jumari, K., & Mirvaziri, H. (2008). Analysis of routing attacks in wireless sensor network. *In Proceedings of International Cryptology Workshop and Conference (Cryptology2008).* (p 202-214). ISBN 978-983-4069

[22] Khalil, I., Bagchi, S., & Shroff, N. B. (2007). Liteworp: detection and isolation of the wormhole attack in static multi-hop wireless networks. *Computer Networks*. Vol 51(15)

[23] Hu, Y. C., Perrig, A. & Johnson, D. B. (2003). Packet leashes: a defense against wormhole attacks in wireless networks. *In IEEE Infocom*

[24] Law, Y. W., & Havinga, P. (2005). How to secure a wireless sensor network. (p 89-95)

[25] Wood, A. & Stankovic, J. (2002). Denial of service in sensor networks. In *Computer*. Vol 35, (p 54 – 62)

[26] Znaidi, W., Minier, M., & Babau, J. P. (2008). An ontology for attacks in wireless sensor networks. *Institut National De Recherche En Informatique Et En Automatique*

Lukman Sharif

Lukman Sharif is a professional member of the Institution of Engineering and Technology (IET). He gained his Bachelor's degree from London Metropolitan University in Computer Networking. He has worked in the IP communications industry for over a decade as a Network Architect and Consultant. He is currently a Senior Lecturer in Computer Networking and Information Security at London College of Research, UK. His research interests include IP routing and security in Mobile Ad-Hoc Networks.

Professor Dr. Munir Ahmed

Professor Dr. Munir Ahmed is a professional member of the Institution of Engineering and Technology (MIET). He is currently pursuing his DProf (Doctorate in Professional Studies) in Computer Communications Engineering Specialisation in Information Security with Middlesex University, London, UK. He earned his PhD in Digital Communications Systems Engineering from London Institute of Technology, London, UK in 1997; his MSc in Information Systems Engineering from London South Bank University, UK in 1994 and BSc in Electrical Engineering from the University of AJK, Kashmir in 1990. Before joining Taibah University as Professor of Computer Networks and Communications Engineering, he was a Professor of Computing and Telecommunications at The American University, London, UK. He has extensive experience in the commercial sector and has held a variety of high-level positions in the industry, including Chief Executive Officer (CEO), Chief Operations Officer (COO), Training Director and Chief Network Architect in the United Kingdom. His current research activities aim to consolidate his skills and extensive commercial experience with various research areas in the field of Computer Networking and Communications Engineering. His particular areas of focus include Wireless Sensor Networks, Mobile Ad-Hoc Networks, Routing Protocols, Network/Information Security and Digital Modulations. Prof. Ahmed is author or co-author of 2 books and more than 20 papers.