Security threats on wireless sensor network protocols

GORINE, Habib <http://orcid.org/0000-0002-7794-6684>

Security Threats on Wireless Sensor Network Protocols

H. Gorine, M. Ramadan Elmezughi

Abstract—In this paper, we investigate security issues and challenges facing researchers in wireless sensor networks and countermeasures to resolve them. The broadcast nature of wireless communication makes Wireless Sensor Networks prone to various attacks. Due to resources limitation constraint in terms of limited energy, computation power and memory, security in wireless sensor networks creates different challenges than wired network security. We will discuss several attempts at addressing the issues of security in wireless sensor networks in an attempt to encourage more research into this area.

Keywords—Malicious nodes, network security, soft encryption, threats, wireless sensor networks.

I. Introduction

WIRELESS sensor networks are composed of large numbers of tiny devices, which are called motes [9]. Each mote has the capability of sensing its environment, computing, and communicating data to other motes until reaching the base station which is linked to cloud storage where data are made available to authorized users.

As can be seen in Fig. 1, a complete wireless sensor network usually consists of a number of sensor nodes for collecting data depending on the application and passes that data to a base station.

Sensor nodes are used to measure physical quantities such as temperature, gas, position, humidity, pressure and so on depending on the application. However, wireless sensor networks have a number of vulnerabilities, which may be exploited by hackers to gain access to the network to steal data or tamper with it [11].

In this paper, we discuss possible security threats for wireless sensor networks and investigate possible solutions.

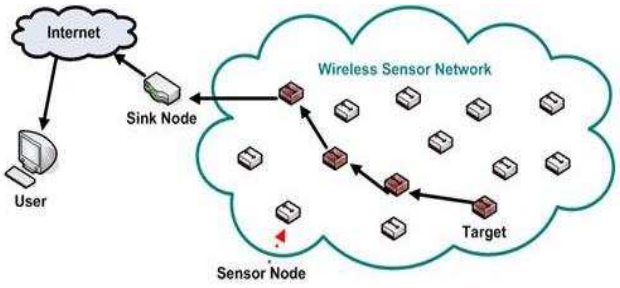

Fig. 1 Wireless Sensor Network Concept

Dr Habib Gorine is a Senior Lecturer and a member of the Network Research Group in the Computing Department at Sheffield Hallam University, Sheffield, United Kingdom (e-mail: h.gorine@shu.ac.uk).

II. Aspects of WSN Security

Wireless sensor networks are a special type of wireless network which share common security requirements with other networks such as confidentiality, integrity, authentication and availability, which need to be addressed during protocol design [7].

- **Data Confidentiality:** Ensures that only authorised sensor nodes can access the content of the collected data. The data may be highly sensitive as in the case of military applications.

The best approach for keeping sensitive data secret is to use symmetric encryption with a secret key that only the intended nodes possess [6].

- **Data Authentication**: Ensures that the data are originated from the correct source. Data authentication allows the receiving node to verify that the data received is sent by a trusted node. For example, in the case of two-node communications, data authentication can be achieved by using a shared secret key to compute the message authentication code of all communicated data.
- **Data Integrity**: Ensures that any received data have not been tampered with by an unauthorized node. For example, a malicious node may add some packets or modify data within a packet before forwarding the corrupt data to its neighbour.
- **Availability :** Ensures that services offered by the whole wireless sensor network or by a single sensor node must be available whenever required.
- **Data Freshness:** Even if confidentiality and data integrity have been achieved it is imperative to ensure that no old data have been replayed. This requirement of fresh data is important when dealing with shared-keys which need to be changed over time.

III. Type of Attacks in WSN

The broadcast nature of wireless sensor networks communication with their limitations in energy, computational power and memory of these tiny sensors, render WSNs susceptible to link attacks ranging from passive eavesdropping to message reply and message modification. The major attacks against wireless sensor networks could be summarised below.

A. Denial of Service Attack (DoS)

In wireless sensor networks, there are several types of DoS attacks depending on the protocol layers [8] as shown below:

Physical layer: DoS attack creates a radio signal that interferes with the radio frequencies being used by the sensor

networks [8] as shown in Fig. 2. Jamming a wireless sensor network can render the entire network inactive and useless.

Data Link Layer: Continually transmitting messages in an attempt to create collisions, which cause the retransmission of the affected packets. This eventually depletes a sensor node's power supply and renders it inactive.

Network Layer: Neglect and greed, misdirection, black hole.

Transport Layer: Malicious flooding by sending many connection requests to a susceptible node, this eventually exhausts the node's resources, thus rendering the node useless.

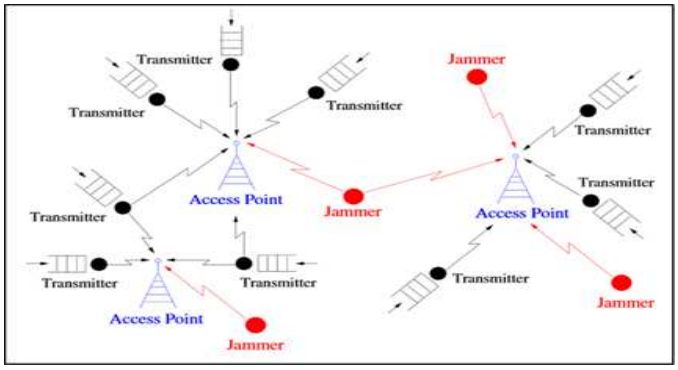

Fig. 2 DoS Attack at the physical layer

B. Sybil Attack

This concept was proposed by Douceur in P2P networks [3] and is defined as a malicious node taking multiple identities to confuse neighbour nodes, causing chaos among them which leads to breakdown of the entire network, as shown in Fig. 1.

Sybil attacks pose a significant threat to geographic routing protocols. During this routing, protocol nodes are required to exchange location information with their neighbours to efficiently route geographically addressed packets. It is reasonable to expect a node to accept a single unique set of coordinates from each of its neighbours. However, using the Sybil attack, an adversary appears to be in more than one place at once.

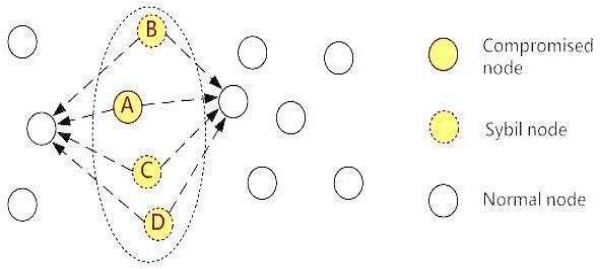

Fig. 3 Sybil node in WSN

C. Selective Forwarding

In a selective forwarding attack, a malicious node may refuse to forward certain packets of data and simply drop them, ensuring that they are not propagated any further.

A simple form of this attack is when a malicious node selectively forwards packets. An attacker suppresses or modifies packets originating from selected nodes and forwards the remaining traffic. Selective forwarding attacks are most effective when the attacker is explicitly included on the data flow path. However, it is possible that an adversary overhearing a flow passing through neighbouring nodes might be able to emulate selective forwarding by jamming each forwarded packet of interest.

D. Blackhole/Sinkhole attack

In a sinkhole attacks, a malicious node acts as blackhole [2] to attract all the traffic in the sensor network through a compromised node creating a metaphorical sinkhole with the adversary at the centre as depicted in Fig. 4.

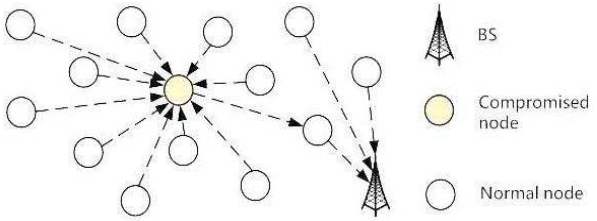

Fig. 4 Blackhole/Sinkhole Attacks

E. Wormhole Attack

One of the most serious attacks in wireless sensor networks is the wormhole attack. It is hard to detect because the attack does not create abnormal traffic into the network [4].

In order to launch a wormhole attack, an adversary connects two distant nodes in the network using a direct low-latency communication link called the wormhole link. As shown in Fig. 5, once the wormhole link is established, the adversary captures data packets at one node (S9) and sends them through the wormhole link to a node another location (S2) and replays them at the other node.

The tunnel creates the illusion that the two end nodes are very close to each other by making tunnelled packets reach the destination node with fewer hops compared to the packets sent over normal routes. This allows an attacker to control several routes within the network and permit or deny data traffic to his advantage.

The counter-measure for the wormhole attack can be implemented at different layers. For example, in this research paper [5], it was suggested using directional antennas at the media access layer and packet leashes at the Network layer. This technique is called 'packet leashes' and overcomes wormhole attacks by restricting the maximum distance of the transmission, using either tight time synchronisation or location information.

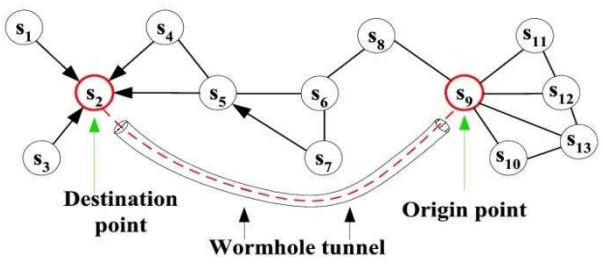

Fig. 5 Wormhole Attack

F. Hello Flood Attack

In Hello Flood Attack, a malicious person uses a laptop with high radio transmission and unlimited power to send HELLO packets to a number of sensor nodes to pretend to be their neighbours. As a consequence, the victim nodes go through the laptop when sending data to the base station and are ultimately spoofed by the attacker as shown in Fig. 6.

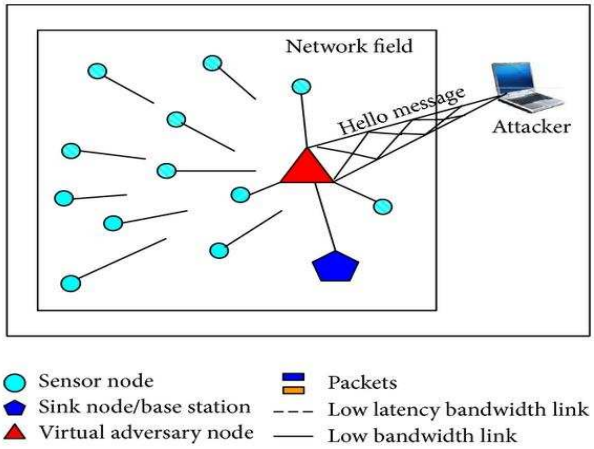

Fig. 6 Hello Flood Attack

IV. Methodology

Three types of research methods are used for evaluating the performance of wireless networks [1]: physical measurement, analytical methods, and network simulation.

In this research paper, a network simulator called ns2 is selected as it is currently the best-known network simulation package for research into wireless networks [10]. NS-2 is written in C++, which uses MIT's Object Tool Command Language (OTcl) as the command and configuration interface.

The simulator is invoked via the ns interpreter and the OTcl scripts defined the simulation rules. NS-2 provides substantial support for the simulation of TCP/ UDP, routing, multicast protocols over both wired and wireless, local and satellite network.

Currently ns-2 is being developed by the Virtual Inter Network Test-bed (VINT) group, which is supported by the Defence Advanced Research Projects Agency (DARPA).

V. Implementation

In this research, a network of 70 sensor nodes operating under the Dynamic Source Routing protocol have been simulated in an area of 700x700m using simulation times of 100, 200, 300, and 500 seconds. During the simulation, the misbehaving nodes were selected randomly at different percentages of the total number of nodes (i.e. 10%, 20%, 30%, 40%, and 50%) which is represented by the horizontal axis of the graphs in Figs. 7-10.

The performance of the network is measured using four parameters (throughput, packet delivery ratio, number of packets dropped and average delay). Each parameter is measured in three separate scenarios:

1. Network under normal operation (i.e. without malicious nodes).
2. Network with deployment of several malicious nodes
3. Network with implementation of soft-encryption to deal with malicious nodes [12].

VI. Results

In this simulation the four parameters (packet delivery ratio (PDR), throughput, packet dropped, average delay) have been measured and results in the form of graphs have been shown below:

A. Packet Delivery Ratio:

From Fig. 7, it is obvious that the performance of the network protocol DSR based on packet delivery ratio is better with soft encryption than without any security mechanism in all the misbehaving nodes.

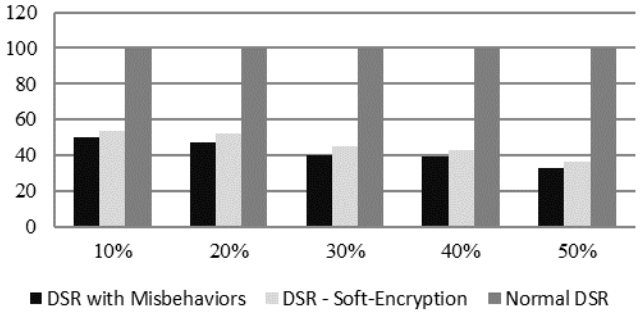

Fig. 7 Packet Delivery Ratio in the three scenarios

B. Throughput:

Fig. 8 shows that the throughput performance metric is slightly better for the DSR with soft encryption than without it.

This improvement is expected because the soft encryption algorithm helps neutralize the effect of misbehaving nodes. However, the DSR performance with soft encryption is still less than the normal DSR.

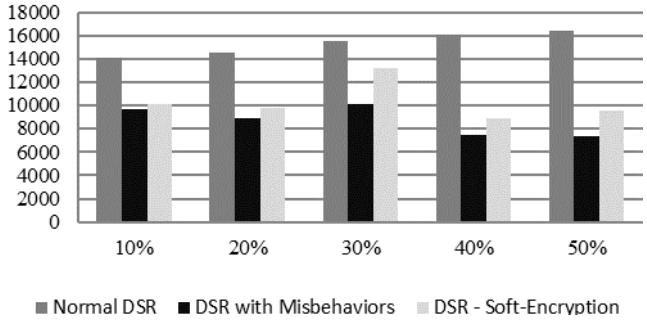

Fig. 8 Throughput measurement in the three scenarios

C. Packets Loss

Fig. 9 shows that the performance DSR regarding packet loss perform better than the DSR without any form of security.

The highest number of packets dropped reached 5732 at 50% of misbehaving nodes, while in the case of DSR without a security solution reached more than 6000 packets at the same rate.

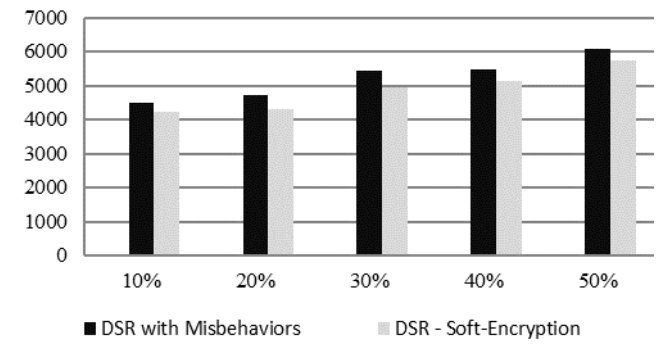

Fig. 9 Packet Loss in the three scenarios

D. Average Delay

Fig. 10 shows interesting results, as the average delay is higher in DSR with soft encryption than without it, which is expected as the algorithm takes time to be executed.

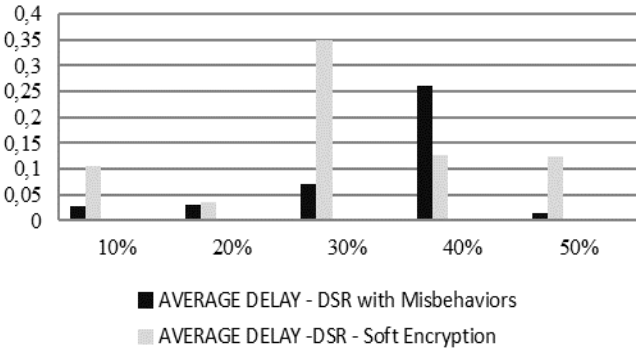

Fig. 10 Average delay in scenario 2 and scenario 3

VII. Conclusion

Security is an important issue in wireless sensor network as hackers are finding new ways to intercept data during their exchange between senor nodes in order to steal or tamper it

In this research, a new security technique called 'soft encryption has been investigated based on trust between sensor nodes.

The performance of the Dynamic Source Routing protocol degrades rapidly with the increase of malicious nodes within the network. However, the implementation of soft-encryption technique proved to detect these malicious nodes and reduces their effect.

References

[1] A. D. Jadhad and P. Goswami, "Evaluating the performance of routing protocols in wireless sensor networks," International Journal of Computer Technology and Electronics Engineering (IJCTEE), 2012, pp. 88-92.

[2] Culpepper, B.J. and Seng, H.C. (2004) "Sinkhole intrusion indicators in DSR MANETs," Proceedings 1stInternational Conference on Broad Band Networks, 2004, pp.681–688.

[3] Douceur, J.R. (2002) "The Sybil Attack," 1st International Workshop on Peer-To-Peer Systems (IPTPS'02), March 2002, LNCS 2429, pp.251–260.

[4] Hu, L. and Evans, D. (2004) "Using Directional Antennas to Prevent Wormhole Attacks," Proceedings of the IEEE Symposium on Network and Distributed System Security (NDSS), 2004.

[5] Perring, A., Hu, L. and D.B. Johnson, D.B. (2003) "Packet Leashes: A Defence against wormhole attacks in wireless sensor networks," Proceedings of 22nd Annual Conference of IEEE Computer and Communication Societies, Vol. 3, April 2003, pp.1976–1986.

[6] Saleh, M. and Khatib, I. A. "Throughput Analysis of WEP Security in Ad-Hoc Sensor Networks," Proceedings, 2nd International Conference on Innovations in Information Technology (IIT05), Sept.26–28, Dubai, 2005.

[7] Singh, S.K., Singh, M.P. and Singh, D.K. "A Survey on Network Security and Attack Defense Mechanism for Wireless Sensor Networks," International Journal of Computer Trends and Technology, May-June Issue, 2001.

[8] Wood, A. D. and Stankovic, J.A. (2002) "Denial of service in sensor networks," IEEE Computer Magazine, vol.5, no.10, Oct. 2002, pp.54–62.

[9] Zheng, J. and Jamalipour, A. (2009), Wireless Sensor Networks: Networking Perspective, published by John & Sons, Inc and IEEE, 2009.

[10] Haddad, I. F. & Gordon, D., 2002. Network Simulator 2: A Simulation Tool for Linux, Linux Journal. (Online) Available at: http://www.linuxjournal.com/article/5929 (Accessed 12 January 2016).

[11] Kavitha, T. Sridharan, D., 2010. Security vulnerabilities in wireless sensor networks: A survey. Journal of information Assurance and Security, 5(1), pp. 31-44.

[12] Yu, Y., Li, K., Zhou, W. & Li, P., 2012. Trust mechanisms in wireless sensor networks: Attack analysis and countermeasures. Journal of Network and Computer Applications, 35(3), pp. 867-880.