DISTRIBUTED RESTRAINING MALWARE PROPAGATION IN MOBILE SINK ROUTING FOR WIRELESS SENSOR NETWORKS

M.Sindhuja[1], A.Komathi[2]

[1]*Mphil Scholar, Department of CS & IT, Nadar Saraswathi College of Arts and Science, (India)*

[2] *Department of CS & IT, Nadar Saraswathi College of Arts and Science, (India)*

ABSTRACT

Advances in wireless sensor network (WSN) technology has provided the availability of small and low-cost sensor nodes with capability of sensing various types of physical and environmental conditions, data processing, and wireless communication. Variety of sensing capabilities results in profusion of application areas. However, the characteristics of wireless sensor networks require more effective methods for data forwarding and processing. In WSN, the sensor nodes have a limited transmission range, and their processing and storage capabilities as well as their energy resources are also limited. Routing protocols for wireless sensor networks are responsible for maintaining the routes in the network and have to ensure reliable multi-hop communication under these conditions. In this paper, we give a survey of routing protocols for Wireless Sensor Network and compare their strengths and limitations.

Keywords: Wireless Sensor Networks, Routing Protocols, Cluster Head

I. INTRODUCTION

Wireless sensor network (WSN) is widely considered as one of the most important technologies for the twenty-first century [1]. In the past decades, it has received tremendous attention from both academia and industry all over the world. A WSN typically consists of a large number of low-cost, low-power, and multifunctional wireless sensor nodes, with sensing, wireless communications and computation capabilities [2,3]. These sensor nodes communicate over short distance via a wireless medium and collaborate to accomplish a common task, for example, environment monitoring, military surveillance, and industrial process control [4]. The basic philosophy behind WSNs is that, while the capability of each individual sensor node is limited, the aggregate power of the entire network is sufficient for the required mission. Although several defense mechanisms [6, 7] have been pro- posed in the literature over the last few years, little work has been done to demonstrate howvulnerable, in terms of data confidentiality and network availability, these networks are. Motivated by this unexplored security aspect, wedemon- strate an attack tool that can be useful not only in highlight- ing the importance of defending sensor networkapplications against attacks but also in studying the effects of these at-tacks on the sensor network itself. This in turn can lead to the development of more secure applications and better detection/prevention mechanisms.

II. ATTACK TOOL ARCHITECTURE OVERVIEW

The attack tool is based on an intelligent component-based system. The hosted components are capable of monitoring any neighborhood traffic, decoding and logging overheard packets, constructing specially crafted messages and launch- ing a number of attacks. Its core functionality is based on three main conceptual modules, as depicted in Figure 1:

• A network sniffer for passive monitoring and logging of radio packets. Any network traffic analysis or packet decoding can be done either in real time or offline through the implemented packet description database.

• A network attack tool that provides a number of actions for compromising a sensor network's security profile. It contains a data stream framework for constructing specially crafted packets that are transmitted by the attack launcher throughout the duration of an attack.

• A network visualization component that visualizes and displays the neighborhood topology, network traffic, node states and status of any performed attack.

The key design goal of this tool is its wide applicability; it should support passive inspection and compromise of a wide variety of sensor network protocols and applications.

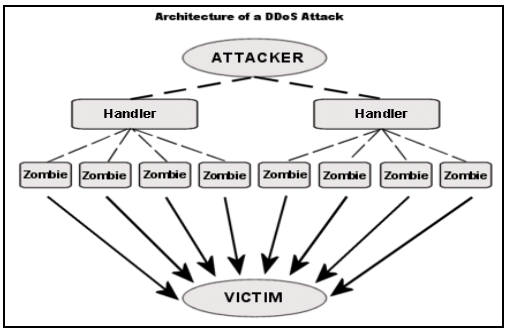

Figure 1: Attack Tool Architecture Layout.

III. NETWORK CONFIDENTIALITY THREATS AND WIRELESS ATTACKS

In wireless networking the overall security objectives remain the same as with wired networks: preserving confidentiality, ensuring integrity, and maintaining availability of information. Thus, identifying risks to sensor networks confiden- tiality posed by theavailability of transactional data is ex- tremelyvital.In an attempt to identify network confidentiality threats, we enhanced our attack tool with a network sniffer for overhear- ing network traffic (Section 3.1). In that way an adversary can process transmitted packets in order to extract vital in- formation such as node IDs or traffic data. Our assertion is that traffic analysis can provide more information about a network'snodes and usage than simply decoding any data packet contents. The presented tool can use carrier frequency to launch a side-channel attack [18] in an attempt to identify the net- work's sensor hardware platform. An adversary could use either a spectrum analyzer or different sensor hardware in combination with our tool in order to detect the current communication frequency. Once the adversary discovers it, she can determine the hardware used and, thus, exploit all the protocol vulnerabilities arising from this specific plat- form. This tool can also compromise a network's confidentiality by monitoring the rate and size of any transmitted/received messages. Specifically, the message rate can reveal infor- mation about the network application and the frequency of monitored events. This constitutes a severe threat since for some sensor applications, like health monitoring, it can lead to a violation of user's privacy. Furthermore, an adversary can examine the rate at which she overhears messages com- ing from a neighborhood and estimate the distance to

the sensed event. Research has shown that the message recep- tion rate increases when the distance to the event reporting node decreases.

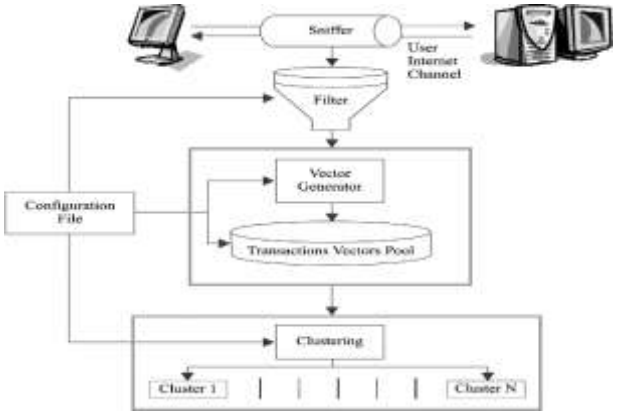

Fig 2. Transactions Vector

3.1 Network Sniffer Component

The network sniffer relies on packets that are overheard in a sensor's node neighborhood. It captures them and logs them for later analysis. Conceptually the sniffer consists of a Local Packet Monitoring module for gathering audit data to be forwarded, over its serial port, to the Packet Storage module for logging at the attached host. This allows offline analysis, through the Packet Description Database, in order to extract vital network information such as node IDs, traffic data or used protocol versions. Essentially, the sniffer enables the construction of a directed graph of all neighboring nodes. Overheard packets flow along the edges of the graph, as

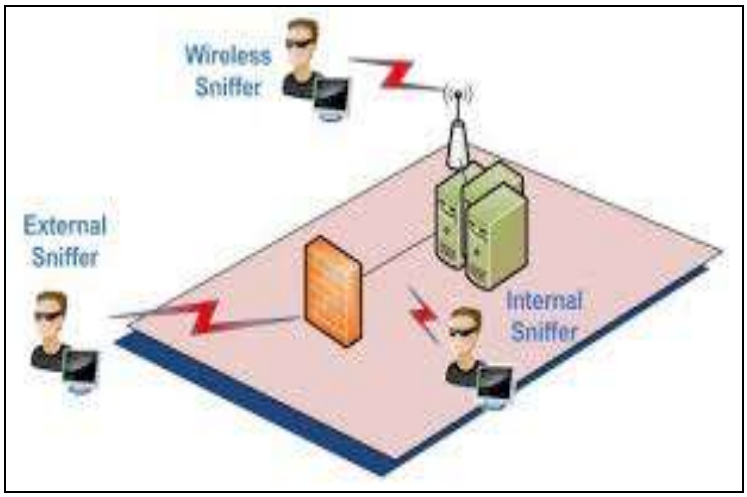

Fig 3. Wireless Network Sniffer

Audit data consist of the communication activities within the sniffer's radio range. Such data can be collected by lis- tening promiscuously to neighboring nodes' transmissions. By promiscuously we mean that when a node is within ra- dio range, the local packet monitoring module can overhear communications originating from that node. Once captured by the radio, all packets are timestamped in order to facili- tate subsequent time-based analysis. Timestamping is per- formed the moment the packet is received by the network sniffer.

3.2 Network Attack Tool Component

This component core functionality is to provide a number of actions for compromising the sensor network's security pro- file. After gathering audit data that are used by the network sniffer to extract vital information and identify the used sen- sor hardware platform and underlying protocols, a user can start launching a number of attacks

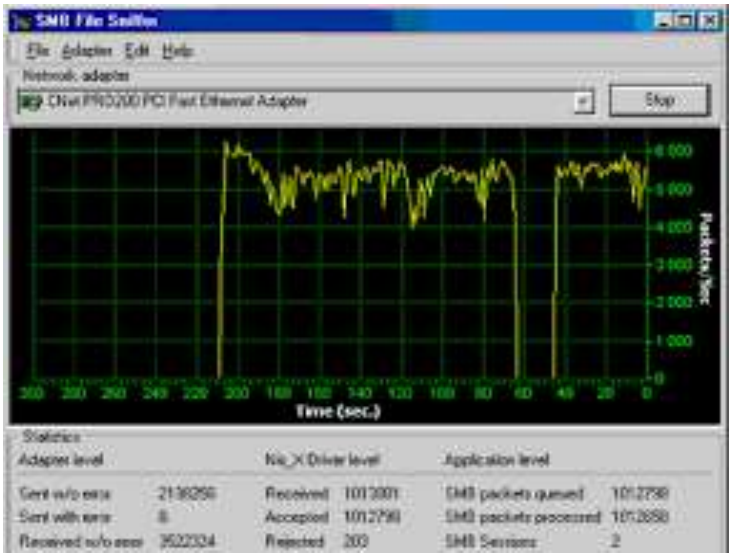

Fig 3.2 (a) Hardware Platform Protocoal

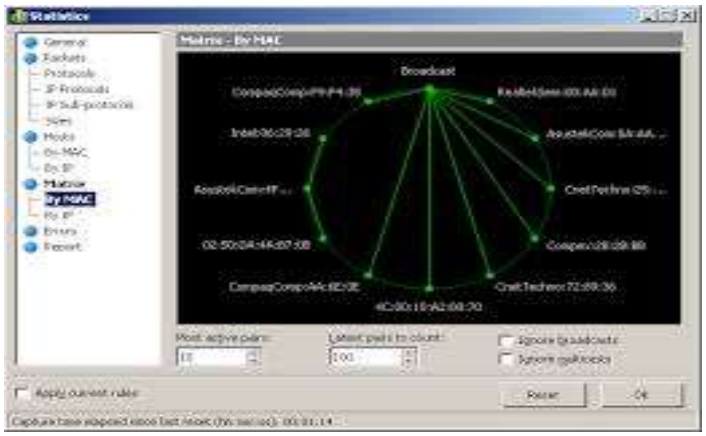

Fig 3.2 (b) List of Supported at- Tacks Can be Found

The resulting network information stream from the packet decoder is fed to the Data Stream Framework of the attack tool component. This data stream processor uses the identi- fied carrier frequency, message size and routing information as its configuration record. All these network characteristics are essential since they are used as the basis for any specially crafted message required by the Attack Launcher.

IV. IMPLEMENTED ATTACKS & ACTIONS

Many sensor network deployments are quite simple, and for this reason they can be even more susceptible to attacks. What makes it particularly easy for attackers is the fact that most protocols are not designed having security threats in mind. As a consequence, they rarely include securityprotection and little or no effort is usually required from the side of an adversary to perform an attack. So, it is very important to study realistic attacker models and evaluate their practicality and effectiveness through a tool as the one presented in this work.

The nature of wireless network communications opens the way to four basic attacks: Interception, Alteration, Disrup- tion and Code or Packet Injection [5]. Most network layer attacks against such networks fall into one of these cate- gories. Our attack tool (in its current version) gives the user the opportunity to perform, in addition to eavesdrop- ping and sniffing, the following actions:

V. CONCLUSIONS

In this paper, we have identified some of the sensor net- works vulnerabilities that can be exploited by an attacker for launching various kinds of attacks. We have demonstrated the practicality of these attacks by building an attack tool for compromising the network's confidentiality and function- ality. The results of this work serve a three-fold purpose: to reveal the vulnerabilities of such networks, to study the ef- fects of severe attacks on the network itself and to motivate a better design of security protocols that can make them more resilient to adversaries. Wireless sensor network security is an important research direction and tools like the current one may be used in coming up with even more attractive solutions for defending these types of networks.

REFERENCES

[1] A. Mainwaring, D. Culler, J. Polastre, R. Szewczyk, and J. Anderson. Wireless sensor networks for habitat monitoring. In WSNA '02: Proceedings of the 1st ACM international workshop on Wireless sensor networks and applications, pages 88–97, New York, NY, USA, 2002. ACM.

[2] J. Tateson, C. Roadknight, A. Gonzalez, T. Khan, S. Fitz, I. Henning, N. Boyd, C. Vincent, and I. Marshall. Real World Issues in Deploying a Wireless Sensor Network for oceanography. In Workshop on Real-World Wireless Sensor Networks REALWSN'05, Stockholm, Sweden, June 2011.

[3] D. Trossen, D. Pavel, G. Platt, J. Wall, P. Valencia, C. A. Graves, M. S. Zamarripa, V. M. Gonzalez, J. Favela, E. Livquist, and Z. Kulcs Sensor networks, wearable computing, and healthcare applications. IEEE Pervasive Computing, 6:58–61, 2007.

[4] A. Becher, Z. Benenson, and M. Dornseif. Tampering with motes: Real-world physical attacks on wireless sensor networks. In J. A. Clark, R. F. Paige, F. Polack, and P. J. Brooke, editors, SPC, volume 3934 of Lecture Notes in Computer Science, pages 104–118. Springer, 2006.

[5] C. Karlof and D. Wagner. Secure routing in wireless sensor networks: Attacks and countermeasures. AdHoc Networks Journal, 1(2–3):293–315, September 2003.