ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 7, July 2018

Real Time attack Detection: An Overview

Shritika Wayker[1], V. L. Kolhe[2]

P.G. Student, Department of Computer Engineering, DYPCOE, Pune, Maharashtra, India[1]

Assistant Professor, Department of Computer Engineering, DYPCOE, Pune, Maharashtra, India[2]

ABSTRACT: Wireless sensor networks have become a mature technology. They are increasingly being used in different practical applications. Examples include the monitoring of industrial environments and light adaptation in tunnels. For such applications, attacks are a serious concern. A disrupted sensor network may not only have a financial impact, but could also be safety-critical. Hence, the key protection is the main goal in attack detection technique. A special challenge lies in fact, that sensor node typically was physically unprotected. Hence, insider attacks are supposed to occur, e.g., by compromising the nodes and getting in possession of the cryptographic keys, thereby becoming a legitimate member of the network. To overcome these shortcomings, this system conduct systematic measurements in a real tested in order to quantify the impact of denial-of-service attacks. It allows identifying those metrics, which was significantly influenced by an attack, and thus appropriate for attack detection. System presents a fully localized intrusion detection system, in which the nodes do not have to collaborate with each other. Based on these results system contains two architectures, allowing the randomization of the detection frequency. The advantage here is, that an adversary may not predict well in advance, which node is responsible to perform intrusion detection at a certain point in time. The gathered data from the extensive measurements is analyzed with statistical approaches. The given intrusion detection systems was evaluated in simulations and prototypical implementations.

KEYWORDS: Wireless Sensor Networks, Intrusion Detection System, DOS, pattern matching algorithm, attack simulation, power consumption, security analysis.

I. INTRODUCTION

In the early 1990's, Mark Weiser introduced a vision called ubiquitous computing, a vision of how system will live and interact with future computing environments. He believed that computers would become almost invisible in use and envisioned the installation of hundreds of wireless computing devices per person. A clear trend in computing is observable: a decrease in size is accompanied by an increase in the number of devices. At the beginning of the computing era, there was one computer, a mainframe, for many people. Later there was one computer, a so-called personal computer, for everyone. Currently, system observes that everyone uses multiple computing devices, such as tablets, mobile phones, and notebooks. This development has been made possible by the invention of small, lightweight, cheap, and mobile processors that used (1) in everyday objects (embedded computing, (2) on the human body (wearable computing), and (3) embedded in the environment (ambient intelligence). System also notices a shift in networking paradigms. Recently, smart things form networks, an example being wireless sensor networks. These networks bridge the gap between the real and the physical world by monitoring the environment with a variety of sensors, such as temperature, humidity, speed, etc. Hence, they show a context-sensitive behaviour and able to remember pertinent events since they have a memory. Single devices communicate over the wireless channel.

II. LITERATURE SURVEY

According to Dandare Punam and Vikrant Chole [1], this approach carried out the detection algorithms for WSN, which detects collision attack based on the packet flow rate to base station node in the wireless network. Simulation results shows that the algorithm have low false toleration and false detection rates and small time to detect attacks.

According to Gomes T. et. Al. [2]. An IoT-based system for collision detection on guardrails system implements an IoT standard stack in order to provide the connectivity and interoperability of the network devices. A Markov Chain model

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 7, July 2018

is used to observe the energy consumption of the given algorithm in each node. An experimental evaluation is also carried out in order to check the theoretical analysis and it was based on the real energy consumption of the developed nodes.

According to Alasseryet. Al. [3], paper explains two techniques that detect compromised nodes in the network that agree to forward packets but fail to do so. In this, key pre-distribution is the form of distribution of keys in contact with nodes before deployment. Therefore, the nodes build up the wireless network using their secret keys in the network after deployment, that is, when they reach their target position. During these stages, secret key is developed, placed in sensor nodes, and each sensor node searches the area in its communication range to find another sensor node to communicate in the network.

According to Miranda J. et. Al. [4], paper explains mechanisms that need the network separate monitoring nodes, specifically one cluster. To monitoring generally means to be fake of the state of that system, to decide a situation for any changes which may occur over during time, using a monitor or measuring device of some sort. Continuous monitoring of each and every other node is not likely for resource-constrained wireless sensor network especially when extending lifetime of the network is the main goal in the layout of WSNs. This given solution, protect WSN from collision attacks.

According to Dhole et. Al. [5], a collaborative reputation system mechanism that has a trust reputation system computes the parameters and publishes reputation scores for a set of objects within an association or domain. Collaborative filtering (CF) is a technique used by some recommender computing systems. Collaborative filtering methods applied to many different kinds of data including: sensing data and monitoring data, such as in mineral exploration. This approach involves continuous monitoring and collecting information about intrusion detections of the system at other places in the network of the area for specific functions. The overhead is too high for WSNs.

According to Yun Ji-Hoon et. Al.[6], a mechanism that disclose act upon nodes by means of observations or reports about several types of collision attacks in the network. An attack is any attempt to destroy, expose, alter, disable, steal or gain illegal access to or make unauthorized use of an asset. This allows nodes to find routes around act upon nodes and to isolate them from the network. An active attack attempts to alter system effects or affect their operation.

III. SYSTEM ARCHITECTURE AND RESEARCH METHODOLOGY

The effect of an attack is different depending of the topology of the network, node software, hardware components or even the node/network configuration. An attack can be very harmful for a specific node but harmless to another node. Thus, the WSN simulation will help to identify the most problematic attacks and which parts of the WSN could be most compromised. With the carried out virtual platform, it is possible to simulate a sufficiently accurate hardware and network model under attack conditions while the real embedded software is being executed in the nodes [13]. With the simulation and performance results, it is possible to identify the most dangerous attacks for the WSN.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 7, July 2018

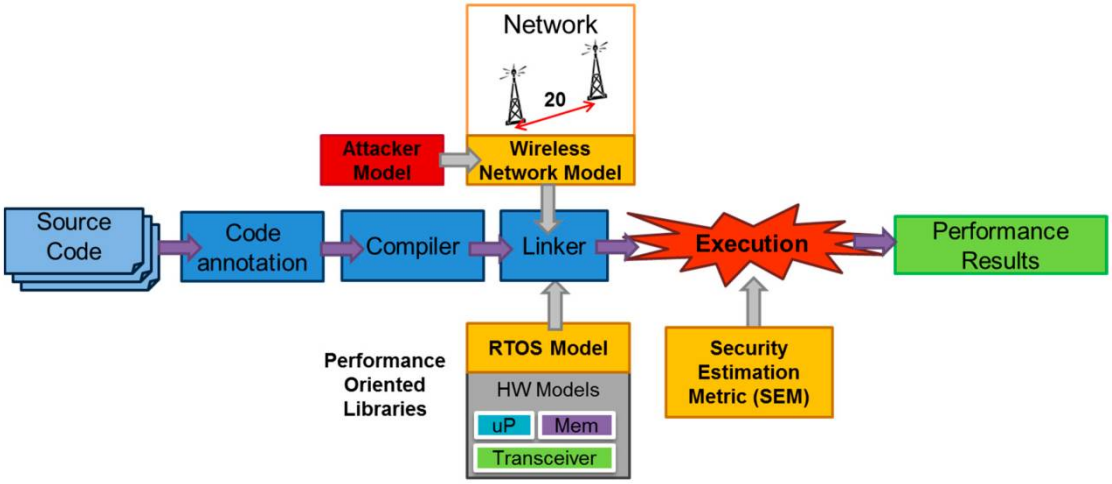

Figure1 : System Architecture [20].

Select a countermeasure: The previous stage enables the detection of the most harmful attacks, thus the next step is to select and evaluate the possible countermeasures. Additionally, it is also possible to use the estimations to modify the embedded software and minimize the attack effect. For this reason, this stage includes two steps:

Design of an attack detection procedure: Once the most dangerous attacks are identified, it is necessary to develop firmware/software that detects when the system is attacked. In order to guide this process, the evaluation of the system behaviour and estimations provided by the WSN simulator used to find the effects that the attacks produce. The objective is to identify a method to detect when a node is being attacked so that a solution to that attack can be implemented. For example, if the network is simulated in normal conditions (without attacks) a rate for the transmitted and received packets can be obtained for a particular network deployment. If the same network is simulated with the injection of a jamming or replication attack, the packet rate in the network and/or in some nodes could change. With the estimations that the virtual simulator provides, the developers can use the attack effect to detect the instant in which an attack takes place. In the case of a jamming attack, the traffic rate varies compared with normal conditions. Because of this variation, it is possible to define a range for normal traffic in a particular deployment. Thus, when this range is violated, the node could assume that it is under attack [20].

Design of attack countermeasures: Once an attack is detected, a countermeasure must be executed. These countermeasures should have minimum effect in the normal behaviour of the network. Moreover, they should avoid the effects that the attacks produce. With these objectives, the software developers can design the countermeasures and test them in the virtual platform, before network deployment. These attack countermeasures may use different techniques. The most common methods include turning off attacked nodes, changing the wireless communication channel, changing the encryption key of the communication messages or even excluding the attacker from the network using a filter. The countermeasures are not limited to these methods but they can be as sophisticated as the developer or application requires. The advantage of the carried out methodology is that these countermeasures can be evaluated and improved before network deployment. Thus, faults and inefficient implementations can be detected in the early stages of the design process and fixed at low cost. In addition, this methodology allows the comparison of different countermeasures, thus only the most efficient is implemented [19].

IV. TYPES OF NETWORK ATTACKS

According different attack detection methodology carried out the signature base anomaly as well as misuse detection in network environment. In this section different authors has define the attack scenario from packet features. Many system had used some network packet filter dataset like ISCX, NSL KDD, KDDCUP99, BOTNET etc.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 7, July 2018

A: Attacks That Introduce Packets in the Network

The first type of attacks was based on the introduction of fake packets into the network with the aim of making the original nodes process them, increasing the traffic in the network and, thus, congesting it or even disrupting the data of the network.

Interrogation attack: This attack exploits the two-way RTS/CTS (Request to Send/Clear to Send) handshake that many media access control (MAC) protocols use to mitigate the hidden-node problem. The attacker repeatedly sends RTS messages to obtain CTS responses from a targeted neighbouring node [20].

Energy Drain: Due to the difficulty of replacing sensor node batteries and their energy constraints, attackers may use compromised nodes to inject fabricated reports into the network or generate large amounts of traffic in the network. These fake messages cause false alarms that waste response effort, and drain the finite amount of energy in a battery-powered network. The aim of this attack is to destroy the sensor nodes in the network, degrade performance of the network and eventually split the network grid up, so taking control of part of the sensor network by inserting a new Sink node [4].

Hello Flood attack: The attacker typically attempts to drain the energy from a node or exhaust its resources. An attacker with large transmission power could broadcast "HELLO" packets (used in many protocols for node discovery) to convince every node in the network that the adversary is within one-hop communication range, causing a large number of nodes to waste energy sending packets to this imaginary neighbour and thus into oblivion [8].

Misdirection attack: The attacker routes the packet from its children to other distant nodes, but not necessarily to its legitimate parent. The main objective of the intruder is to misdirect the incoming messages to increase the latency, which prevents a few packets from reaching the base station [19]. **Flooding attack:** An attacker may repeatedly make new connection requests until the resources required by each connection exhausted or a maximum limit is reached. It produces severe resource constraints for legitimate nodes [8].

B: Attacks That Introduce Noise in the Network

The effects of the attacks placed in this group consist in reducing the traffic in the network. These attacks are focused on the introduction of noise in the network (or other techniques) with the objective of increasing the probabilities of packet loss. The main consequence of these attacks is the increment in the packet loss rate which can disrupt the proper function of the network. The attacks placed in this category are the following:

Jamming attack: This works by denying service to authorized users as legitimate traffic is jammed by the overwhelming amount of illegitimate traffic. It disrupts network functionality by broadcasting high-energy signals [17].

Collision attack: In a collision attack, an attacker node does not follow the medium access control protocol and produces collisions with the neighbouring node's transmissions by sending a short noisy packet. Packets collide when two nodes attempt to transmit on the same frequency simultaneously, producing packet corruption. This attack can cause a lot of disruption to network operation [1].

Resource Exhaustion attack: Operation of this attack consists in repeated collisions and multiple retransmissions until the node dies. A malicious node continuously requests or transmits over the channel [16].

Black Hole attack: A black hole attack basically consists in the network routing alteration with the objective of attracting all the packets to the attacked node destination, and silently discarding or dropping them [11].

Denial of service (DoS) attacks: In a Path-based DoS (PDoS) attack, an adversary swamps sensor nodes a long distance away by flooding a multihop end-to-end communication path with either replicated packets or spurious injected packets. It can cause serious damage in resource-constrained systems [10].

Homing attack: In a homing attack, the attacker looks at network traffic to deduce the geographic location of critical nodes, such as cluster heads or neighbours of the base station. The attacker can then physically disable these nodes. This leads to another type of black hole attack [5].

Selective Forwarding attack: Multi-hop networks assume that participating nodes will faithfully forward and receive messages. However a malicious node may refuse to forward certain messages and simply drop them, ensuring that they are not propagated any further. The procedure to launch selective forward attacks is very similar to the black hole one. First, a malicious node has to convince the network that it is the nearest node to the base station, attracting network traffic to route data through it. Then, a selection of packets is dropped [13].

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 7, July 2018

C: Attacks That Modify the Firmware of a Node

Finally, some attacks do not directly affect the network traffic but they could affect the software/firmware or the hardware of the node. These attacks usually require direct access to the hardware node (tamper attacks).

Application attack: This attack modifies the firmware/software that is stored in a node. It normally requires access to the on-field software update procedure (Over the Air Programming procedure) or physical access to the hardware of the node [14] .
Overwhelm attack: An attacker might attempt to overwhelm sensor nodes with sensor stimuli that could produce large volumes of traffic to a base station. This induces, among other problems, a power consumption increase in the attacked nodes and the generation of unreliable sensor info [15].

V. RESULTS AND DISCUSSIONS

Basically the overall analysis has categorised into Network base Intrusion Detection System (NIDS) as well as Host base Intrusion Detection System (HIDS). Table the each attack detection accuracy with class wise, which is achieved in existing experiments.

Table 1 : Attack detection accuracy for each sub attack

Congesting base Attacks	Interrogation Attack [20]	75%
	Energy Drain Attack [4]	89%
	Misdirection Attack [19]	85%
	Hello Flood Attack [8]	90%
	Flooding Attack [8]	87%
Tamper Attacks	Application attack [14]	80%
	Overwhelm attack [15]	82%
Flooding / Noise base Attacks	Resource Exhaustion attack [16]	60%
	Jamming Attack [17]	82%
	Collusion Attack [1]	91%
	Black Hole Attack [11]	86%
	DOS Attack [10]	98%
	Homing attack [5]	95%
	Selective Forwarding attack [13]	92%

Figure 2 shows the classification accuracy of different class attacks. The overall accuracy shows as average detection ratio for all attacks. In all existing works most of systems had used training and testing modules for achieve the maximum detection accuracy. NSL KDD, KDD CUP99, ISCX, Network sniffer dataset has used in experiment analysis by all the systems.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 7, July 2018

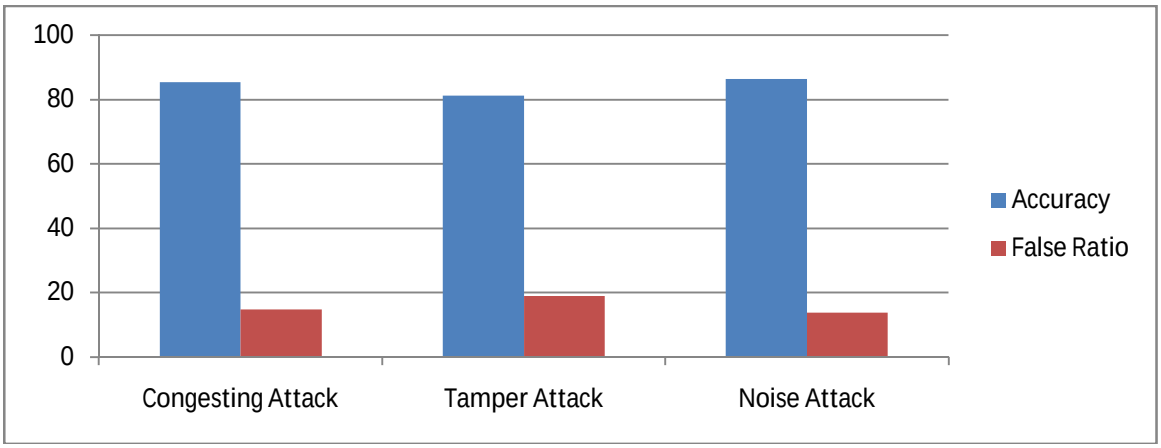

Figure 2 : Attack Classification Accuracy

VI. CONCLUSION

This paper analyses the characteristics of wireless sensors network, and in order to recover the threat of collision attack in the network, for there are some external attack and internal attack in wireless sensor networks. Providing security in wireless sensor networks during operation involves addressing multiple challenges, especially the reduction of complexity and resource requirements in intrusion detection. Throughout this overview, used many techniques for accurate detection as well as prevention.

REFERENCES

[1] Dandare, Punam, and Vikrant Chole. " Detection of Collision Attacks and Comparison of Efficiency in Wireless Sensor Network." International Journal Of Engineering And Computer Science 5.5 (2016).
[2] Gomes, T., et al. "An IoT-based system for collision detection on guardrails." Industrial Technology (ICIT), 2016 IEEE International Conference on.IEEE, 2016.
[3] Alassery, Fawaz, et al. "Collision Detection in Wireless Sensor Networks Through Pseudo-Coded ON-OFF Pilot Periods per Packet: A Novel Low-Complexity and Low-Power Design Technique." Computer and Information Science 8.3 (2015): 13.
[4] Miranda, J., et al. "A wireless sensor network for collision detection on guardrails. " Industrial Electronics (ISIE), 2014 IEEE 23rd International Symposium on.IEEE, 2014.
[5] Dhole, Miss Komal V., and A. S. Dhudhe. "Effective Vehicle Collision Detection System by Using Vehicular Ad-Hoc Network." (2017).
[6] Yun, Ji-Hoon, and Seung-Woo Seo. "Novel collision detection scheme and its applications for IEEE 802.11 wireless LANs." Computer Communications 30.6 (2007): 1350-1366.
[7] Tay, Y. C., Kyle Jamieson, and HariBalakrishnan. "Collision-minimizing CSMA and its applications to wireless sensor networks."IEEE Journal on selected areas in Communications 22.6 (2004): 1048-1057.
[8] Stathopoulos, Thanos, et al. "Application-based collision avoidance in wireless sensor networks." Local Computer Networks, 2004.29th Annual IEEE International Conference on.IEEE, 2004.
[9] Chockler, Gregory, et al. "Consensus and collision detectors in wireless ad hoc networks." Proceedings of the twenty-fourth annual ACM symposium on Principles of distributed computing. ACM, 2005.
[10] McCune, Jonathan M., et al. "Detection of denial-of-message attacks on sensor network broadcasts." Security and Privacy, 2005 IEEE Symposium on.IEEE, 2005.
[11] B.-H. Chen and S.-C. Huang, "An advanced moving object detection algorithm for automatic traffic monitoring in real-world limited bandwidth networks," IEEE Trans. Multimedia, vol. 16, no. 3, pp. 837–847, Apr. 2014.
[12] B. Pan, U. Demiryurek, and C. Shahabi, "Utilizing real-world transportation data for accurate traffic prediction," in Proc. IEEE 12th Int. Conf. Data Mining (ICDM), 2012, pp. 595–604.
[13] B. Pan, U. Demiryurek, C. Gupta, and C. Shahabi, "Forecasting spatiotemporal impact of traffic incidents on road networks," in Proc. IEEE13th Int. Conf. Data Mining (ICDM), 2013, pp. 587–596.
[14] A. T. Baptista, E. P. Bouillet, and P. Pompey, "Towards an uncertainty aware short-term travel time prediction using GPS bus data: Case study in Dublin," in Proc. IEEE 15th Int. Conf. Intell. Transp. Syst. (ITSC), Sep. 2012, pp. 1620–1625.
[15] M. Fire, D. Kagan, R. Puzis, L. Rokach, and Y. Elovici, "Data mining opportunities in geosocial networks for improving road safety," in Proc. IEEE 27th Conv. Elect. Electron. Eng. Israel (IEEEI), Nov. 2012, pp. 1–4.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 7, July 2018

[16] P. Zhou, Y. Zheng, and M. Li, "How long to wait? Predicting bus arrival time with mobile phone based participatory sensing," IEEE Trans. Mobile Comput., vol. 13, no. 6, pp. 1228–1241, Jun. 2014.
[17] E. Koukoumidis, M. Martonosi, and P. Li-Shiuan, "Leveraging smartphone cameras for collaborative road advisories," IEEE Trans. Mobile Comput., vol. 11, no. 5, pp. 707–723, May 2012.
[18] R. Fracchia and M. Meo, "Analysis and design of warning delivery service in intervehicular networks," IEEE Trans. Mobile Comput., vol. 7, no. 7, pp. 832–845, Jul. 2008.
[19] J. White, C. Thompson, H. Turner, B. Dougherty, and D. C. Schmidt, "Automatic traffic accident detection and notification with smartphones," Mobile Netw. Appl., vol. 16, no. 3, pp. 285–303, Jun. 2011.
[20] Diaz, A.; Sanchez, P. Simulation of Attacks for Security in Wireless Sensor Network. *Sensors* 2016, *16*, 1932.