www.ijecs.in
International Journal Of Engineering And Computer Science ISSN: 2319-7242
Volume 5 Issue 5 May 2016, Page No. 16400-16406

Detection of Collision Attacks and Comparison of Efficiency in Wireless Sensor Network

Punam Dandare[1], Prof. Vikrant Chole[2]

[1]Department of Computer Science and Engineering,
G. H. Raisoni Academy of Engineering and Technology, Nagpur, India
punam170592@gmail.com

[2] Department of Computer Science and Engineering,
G. H. Raisoni Academy of Engineering and Technology, Nagpur, India
vikrant.chole@raisoni.net

Abstract: ***Wireless sensor networks (WSNs) consist of sensor nodes. It is a collection of wild number of low cost device constraint sensor nodes that communicates using wireless medium and they are small in size, low battery power and limited processing capability. This restraint of low electricity power of a sensor node and limited energy capability makes the wireless sensor network failure. Thus, data aggregation is very important techniques in wireless sensor networks and it reduces the energy consumption by eliminating redundancy. The increased deployment of ubiquitous WSN networks has exponentially increased the complexity to detect WSN attacks and protect in oppose to them. In this paper, we consult that collision attack in a network that can be easily launched by a hostile node: a hostile node does not follow the medium access control protocol and purpose collisions attack with neighbor communication by sending a short noise packet. Collision attack means the formation of nodes to access the false data. The data collected from singular nodes is aggregated at a base station or host computer. This attack does not consume much more energy of the attackers but can cause a lot of disruption of the network operation. Due to the wireless broadcast nature, it is not insignificant to identify the attacker. This paper specifies detection algorithms for WSN, which detects collision attack based on the packet flow rate to base station node in the wireless network. Simulation results show that the algorithm have low false toleration and false detection rates and small time to detect attacks.***

Keywords: Data Aggregation, Wireless sensor network, Cluster head, Privacy, Collision attack, Packet flow, Cluster topology

1. Introduction

A wireless sensor network consists of a collection of the nodes that have the facility to sense, process data and communicate with each sensor node via a wireless connection. WSNs, the improvement in sensor technology has made it possible to have very small device, low powered sensing devices that capable with programmable compute, multiple parameter. Also, the low cost device makes it possible to have a network of hundreds or thousands of these sensors, thereby enhancing the flexibility and accuracy of data in a network and the area coverage.

This project presents a new refined collusion attack scenario oppose a number of existing Iterative Filtering (IF) algorithms based on the incorrect data injection. In such an attack scenario, attacker attempt to alter the aggregate value by forcing such collision algorithms to converge to skewed values. In this paper, we propose a solution for susceptibility by providing an initial trust reputation system estimate which is based on a robust estimation of errors of individual sensors. Establishment of a new collusion attack against iterative filtering based reputation systems which reveals a severe vulnerability of IF algorithms.

Wireless sensor networks are composed of many low cost micro sensor nodes which are expand in the control area. In network area, each sensor node can form a multi-hop clustering self-organizing network through wireless communication, and each sensor node is able of sensing, data processing and communication [1]. Generally speaking, wireless sensor network is often expanding in an open environment of network, even the enemy-occupied domain. As sensor nodes transfer network data through wireless communication link in a network area, the network can be easily captured and invaded. Due to the lack of foundation framework like wired network, what wireless sensor networks face not only traditional security

threats but also some collision attacks which include the exhaustion attack, selective forwarding-attack, wormhole-attack, collision attack, sinkhole-attack, etc. Besides, each sensor node has limited energy and processing capability, small storage space and low bandwidth, this put ahead a larger challenge for the security of wireless network. In this work, we focus on collision Attack in a network [2]. In the collision attack, in cryptography, a collision attack on a cryptographic hash function tries to find two input data producing the same hash value, i.e. a hash collision. In contrast to a pre image attack the hash value is not specified.

In theory, causing collisions in only one byte is enough to create a cyclic redundancy code error and to injure the message. The advantages of a collision attack are the short power energy consumed and to detect it (the only evidence of collisions attacks is incorrect message). Collisions are certain whenever members of a very large set (such as all possible person names, or all possible computer data) are mapped to a relatively short bit string. This is merely an instance of the pigeonhole principle. The impact of collisions depends on the application. Checksums, on the other hand, are designed to minimize the probability of collisions in between similar input data in a network area, without regard for collisions between very different inputs.

2. Literature review

Marti, S., Giuli, T. J., Lai, K., and Baker, M., et al. [3] presented two techniques that detect compromised nodes in the network that agree to forward packets but fail to do so. In this, key predistribution 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 keys are 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. A secure link layer is established when two nodes detect one or more common keys, and network communication is done on that link in the network between those two nodes.

Buchegger, S. and Le Boudec, J. et al. [4] proposed 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. Any kind of malicious activity that attempts to collect disrupts, deny or destroy information system resources or the information itself. An active attack attempts to alter system effects or affect their operation. A passive attack attempts to learn or use of information from the system but does not affect system effects. An attack can be execute by an insider or from outside the organization. The overhead is prohibitive for WSNs.

Michiardi, P. and Molva, R., et al. [5] present 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.

Chen, Z. and Khokhar, Huang et al. [6] present 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. Network monitoring is the use of a system data that monitors a computer network for slow or failing a component of that network and that notifies the network administrator. It is part of network management.

All the above way monitor individual nodes all the time. 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. Our proposed solution, protect WSN from collision attacks.

3. Proposed Work

A wireless sensor network communication channel is open in air, so attacking it is not a difficult task. Some of the attack scenarios against WSN are:

Eavesdropping, data injection, and traffic analysis attacks;

Denial of service attacks;

3.1 Typical Threats in WSNs

The threats and adequate defense techniques in WSNs can be classified as in Table 1.

Table 1: The threats and adequate defense techniques in WSNs

Threat	Layer	Defense techniques
Jamming	Physical Layer	Spread-spectrum, lower duty cycle
Tampering	Physical Layer	Tamper-proofing, effective key management schemes
Exhausting	Link Layer	Rate limitation
Collision	Link Layer	Error correcting code
Route information. Manipulating	Network Layer	Authentication, encryption
Selective forwarding	Network Layer	Redundancy, probing
Sybil attack	Network Layer	Authentication
Sinkhole	Network Layer	Authentication, monitoring, redundancy
Wormhole	Network Layer	Flexible routing, monitoring
Hello flood	Network Layer	Two-way authentication, three-way handshake
Flooding	Transport Layer	Limiting connection numbers, client puzzles
Clone attack	Application Layer	Unique pair-wise keys

3.2 Packet Traffic Arrival Process

Packet traffic is the process of jamming in the network, because the data traffic dynamics in different WSN scenarios are quite different, the data traffic modeling and analysis in WSNs will be quite application dependent. In [13] it is suggested that WSN applications can be categorized as event-driven or periodic data generation. A network packet is a formatted unit of data carried by a packet-switched network. Computer communications links that do not support packets, such as traditional point-to-point telecommunications links, simply transmit data as a bit stream. When data is formatted into packets, the bandwidth of the communication medium can be better shared among users than if the network were circuit switched.

A packet consists of control information and user data, which is also known as the payload. Control information provides data for delivering the payload, for example: source and destination network addresses, error detection codes, and sequencing information. Typically, control information is found in packet headers and trailers. Different communications protocols use different conventions for distinguishing between the elements and for formatting the data. For example, in Point-to-Point Protocol, the packet is formatted in 8-bit bytes, and special characters are used to delimit the different elements. Other protocols like Ethernet, establish the start of the header and data elements by their location relative to the start of the packet. Some protocols format the information at a bit level instead of a byte level. For periodic data generation scenarios, constant bit rate (CBR) can be used to model the data traffic arrival process when the bit rate is constant [14]. Constant bitrate (CBR) is a term used in telecommunications, relating to the quality of service. Compare with variable bitrate. When referring to codecs, constant bit rate encoding means that the rate at which a codec's output data should be consumed is constant. CBR is useful for streaming multimedia content on limited capacity channels since it is the maximum bit rate that matters, not the average, so CBR would be used to take advantage of all of the capacity. CBR would not be the optimal choice for storage as it would not allocate enough data for complex sections (resulting in degraded quality) while wasting data on simple sections. The problem of not allocating enough data for complex sections could be solved by choosing a high bitrate to ensure that there will be enough bits for the entire encoding process, though the size of the file at the end would be proportionally larger. When the bit rate is variable, a Poisson process can be used to model the data traffic arrival process as long as the data traffic is not bursty [15]. In telecommunication, the term burst transmission or data burst has the following meanings:

- Any relatively high-bandwidth transmission over a short period. For example, a download might use 2 Mbit/s on average, while having "peaks" bursting up to, say, 2.4 Mbit/s.
- Transmission that combines a very high data signaling rate with very short transmission times, and the message is compressed. That is popular with the military and spies, who both wish to minimize the chance of their radio transmissions being detected, a low probability of intercept (LPI) and low probability of recognition (LPR).
- To transmit large amounts of primarily textual information: they would display multiple pages of text in rapid succession, usually at the end of the programme; viewers would videotape it and then read it later by playing it back using the pause button after each page.
- Operation of a data network in which data transmission is interrupted at intervals.

A Poisson process has also been used to model the traffic arrival process in an event-driven WSN [16]. However, there is no solid ground to support the use of a Poisson process in this case. Actually, the widely used Poisson processes are quite limited in their burstiness [17]. Brstiness is the intermittent increases and decreases in activity or frequency of an event. One of measures of burstiness is the Fano factor—a ratio between the variance and mean of counts. Burstiness is observable in natural phenomena, such as natural disasters, or other phenomena, such as network/data/email network traffic or vehicular traffic. Burstiness is, in part, due to changes in the probability distribution of inter-event times. Distributions of bursty processes or events are characterized by heavy. Burstiness of inter-contact time between nodes in a time-varying network can decidedly slow spreading processes over the network. This is of great interest for studying the spread of information and disease.

3.3 Protection Algorithms

The system is a cluster type of intrusion detection for wireless sensor networks. The MD5 message-digest algorithm is a extensively used cryptographic hash function producing a 128-bit (16-byte) hash value, typically assets in text format as a 32-digit hexadecimal number. MD5 has been utilized in a wide variety of cryptographic applications and is also commonly used to justify data integrity. MD5 is a one-way function; it is neither encryption nor encoding. For security and protection of data we use Md5 (message Digestion) algorithm is used:

In this system, at first, we make the following assumptions:

- In the network area, each sensor node has the same resources and energy constrained, between nodes is equivalent.
- The node is dynamic in network, and the detection area is divided into clusters by the clustering algorithm, and clustering algorithm can automatically run on the basis of the conditions of network set by the algorithm.
- The common node of each cluster can directly communicate with the cluster head node or aggregator node or communicate through multi-hop cluster head.
- The base station is a safe and unlimited resources, and can communicate with each unify elected cluster head node, it can form a new cluster with all the cluster head node based the base station on cluster head.

3.4 Packet Transmission in WSN Serves As The Data Source Of Anomaly Detection

Packet traffic has been the most used data source in the anomaly detection for WSNs. The transmission time, is the amount of time from the beginning until the end of a message transmission in the network. In the case of a digital message, it is the time from the first bit until the last bit of a message has left the transit data node. The packet transmission time in seconds can be obtained from the packet size in bit and the bit rate in bit/s as:

Packet transmission time = Packet size / Bit rate;

The authors propose that an anomaly in wireless sensor network could disrupt one of the following rules applied to packet traffic:

1) Interval rule: A failure is raised if the time that which passes between the sources of two consecutive messages is larger in size or smaller than the allowed limits.

2) Retransmission rule: Network protocols that use aggressive retransmissions to refund for packet loss due to collision can increase congestion, even after the initial load has been reduced to a level of area that would not normally have convinced network congestion. Such networks exhibit two stable states under the same level of load balance. The stable state with low throughput is known as congestive collapse.

3) Integrity rule: The message payload of the system must be the same along the path from its origin to a destination, considering that in the retransmission process of data there is no data aggregation by other sensor nodes.

4) Delay rule: The retransmission of a message by a monitor's neighbor must occur before a defined timeout. In a network based on packet switching, transmission delay is the amount of time required to push all the packet's bits into the wire. This delay is proportional to the packet's length in bits.

It is given by the following formula by using delay rule:

$$D_T = N/R_{\text{seconds}}$$

where

D_T is the transmission delay in seconds
N is the number of bits, and
R is the rate of transmission in the network (say in bits per second)

5) Repetition rule: The same message can be retransmitted by the same neighbor in the network only a limited number of times.

6) Radio transmission range: In Radio transmission, all messages listened to by the monitor must have originated (previous hop) from one of its neighbors. The protocols that neglect congestive collapse are based on the idea that data loss is caused by congestion in the network.

7) Jamming rule: The number of collisions attacks associated with a message sent by the monitor must be lower than the expected number in the wireless network. By regularly monitoring to the violations of the listed rules, network anomalies will be detected.

4. Experimental Results

4.1 Simulation parameters:

Ns-2 simulator will be used to evaluation our work. Ns-2 is an object-oriented (OO) programming simulator, written in C++ language, with an OTCL interpreter as a front-end. Simulation kernel, models, protocols, i.e UDP or TCP and other components are implemented in C++ language, but are also accessible from OTcl. OTcl usually refers to an object oriented extension of Tcl .OTcl is scripting language. OTCL is used for simulator configuration, setting up network topology, specifying scenarios of framework, recording simulation results etc. Typical ns-2 OTcl script for wireless simulation begins with configuration tool command, which is used to specify PHY, MAC and routing protocol, radio propagation and antenna model, topology for network etc. The next step is creation of mobile nodes. Node movement and network traffic patterns are usually defined in separate files in database. Tools for generating these files are provided. The table 2 shows the simulation parameters:

Table 2: Simulation Result

channel type	Wireless Channel
radio-propagation model	Propagation/Two Ray Ground
network interface type	Phy/Wireless Phy/802_15_4
MAC type	Mac/802_11
interface queue type	Queue/DropTail/PriQueue
link layer type	LL
antenna model	Antenna/Omni Antenna
max packet in ifq	1000
number of sensor nodes	24
protocol type	AODV
X dimension of topography	900
Y dimension of topography	900
simulation period	15.0 min
number of CH (cluster head) nodes	3
number of base station node	1

5. Results

The analysis of comparative parameters ratio are shown in Table 3.

Table 3: Analysis of comparative parameters ratio

Generated Packet	Received Packet	Packet Delivery Ratio	Average end-to-end delay	Dropped packet
707	410	57.9915	42.0085 msec	297

The various comparative graphs are as follows:

DOI: 10.18535/ijecs/v5i5.13

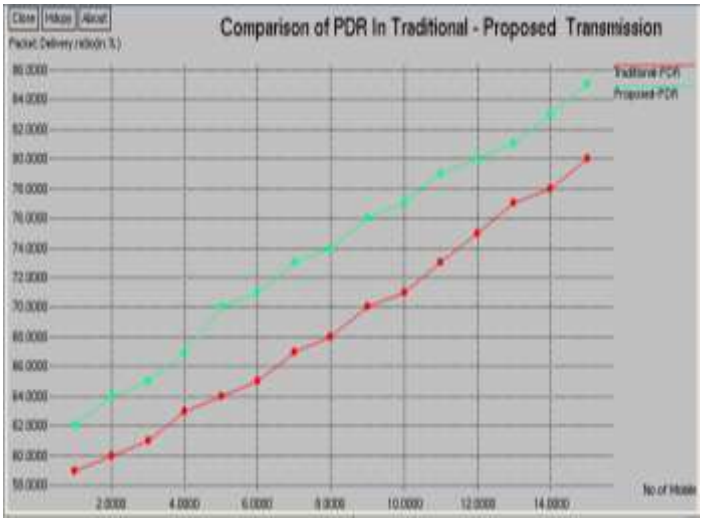

Figure 1: Comparison of Packet delivery ratio

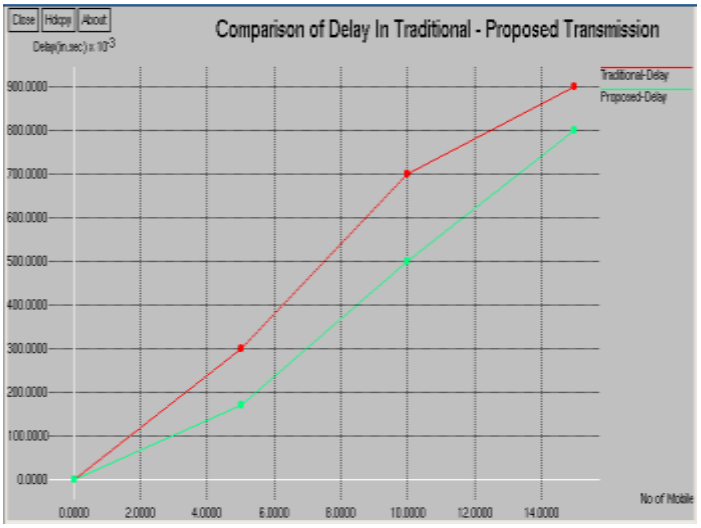

Figure 2: Comparison of Delay

Figure 3: Report Performance on false data

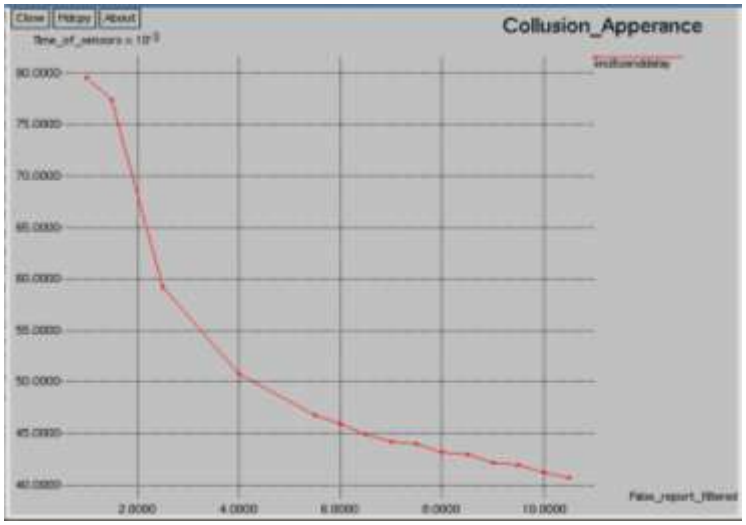

Figure 4: Collision Appearance on false data

6. Conclusion

This paper analyzes 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, we proposed algorithm for wireless sensor networks based on collision and packet flow rate. Our algorithms no needing additional requirements, because they are made in base station. Building on the simulation results, our algorithms are Very effective. By using collision algorithm, we detect attacks and maintain security by using security algorithm.

References

[1] Zhenwei Yu, Jeffrey J.P. Tsai,A Framework of Machine Learning Based Intrusion Detection for Wireless Sensor Networks, IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing,2008.

[2] W. Znaidi, M. Minier and J. P. Babau; An Ontology for Attacks in Wireless Sensor Networks; INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET EN AUTOMATIQUE (INRIA); Oct 2008.

[3] Marti, S., Giuli, T. J., Lai, K., and Baker, M., .Mitigating Routing Misbehavior in Mobile Ad Hoc Networks,. Proc. 6th Annual Intl. Conf. on Mobile Computing and Networking (MobiCom.00), Boston, Massachusetts, August 2000, pp. 255-265.

[4] Buchegger, S. and Le Boudec, J., .Performance Analysis of the CONFIDANT Protocol: Cooperation of Nodes -Fairness in

Dynamic Ad-hoc Networks., Proc. 13th IEEE/ACM Symp. on Mobile Ad Hoc Networking and Computing (MobiHoc), Lausanne, Switzerland, June 2002.

[5] Michiardi, P. and Molva, R., .CORE: A collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks., Proc. IFIP 6th Joint Working Conference on Communications and Multimedia Security (CMS.02), Portoro., Slovenia, September 2002, pp. 107-122.

[6] Chen, Z. and Khokhar, A., "Self Organization and Energy Efficient TDMA MAC Protocol by Wake Up For Wireless Sensor Networks", Proc. First Annual IEEE Intl Conf. on Sensor and Ad Hoc Communications and Networks (SECON 2004), Santa Clara, CA, October 2004.

[7] Demirkol, I., Alagoz, F., Delic, H., and Ersoy, C. (2006). Wireless sensor networks for intrusion detection: Packet traffic modeling. IEEE Communications Letters, 10(1):22--24.],

[8] Cui, S., Madan, R., Goldsmith, A. J., and Lall, S. (2005). Joint routing, mac, and link layer optimization in sensor networks with energy constraints. In Proc. of IEEE International Conference on Communications (ICC'05), pages 725--729.

[9] Ma, Y. and Aylor, J. H. (2004). System lifetime optimization for heterogeneous sensor networks with a hub-spoke topology.

IEEE Transactions on Mobile Computing, 3(3):286--294.

[10] Tang, S. (2006). An analytical traffic flow model for cluster-based wireless sensor networks.In Proc. of 1st International Symposium on Wireless Pervasive Computing.

[11] Paxson, V. and Floyd, S. (1995). Wide-area traffic: The failure of poisson modeling. IEEE/ACM Transactions on Networking, 3:226--244.

[12] Wang, Q. and Zhang, T. (2008). Source traffic modeling in wireless sensor networks for target tracking. In Proc. of the 5th ACM International Symposium on Performance Evaluation of Wireless Ad-Hoc, Sensor, and Ubiquitous Networks (PE-WASUN'08), pages 96--100.

[13] Wang, P. and Akyildiz, I. F. (2009). Spatial correlation and mobility aware traffic modeling for wireless sensor networks.In Proc. of IEEE Global Communications Conference (Globecom'09).

[14] W. Lee, S. J. Stolfo K. Mok, "A data mining framework for building intrusion detection models", In Proc. IEEE Symposium on Security and Privacy, 1999.

[15] SJ Stolfo, W Lee, PK Chan, W Fan, E Eskin "Data mining-based intrusion detectors: an overview of the columbia IDS project" ACM SIGMOD Record, 2001 -portal.acm.org.

[16] Lippmann et al. "Evaluating intrusion detection systems: The 1998 DARPA offline intrusion detection evaluation", In Proceedings of the on DARPA Information Survivability Conference and Exposition (DISCEX'00).

[17] J. McHugh. Testing intrusion detection systems: A critique of the 1998 and 1999 DARPA intrusion detection system evaluations as performed by Lincoln Laboratory.

[18] K. Fall and K. Varadhan, "The ns manual", User's manual, UC Berkeley, LBL, USC/ISI, and Xerox PARC, January 2009.