Survey on Delay Attack Detection and Prevention in WSN Data Transport

Bhushan Jichkar, Prof. D. C. Mehetre

Abstract— Wireless Sensor Network (WSN) is a large network of sensor nodes. Wireless Sensor Networks are very popular and have their special characteristics such as limited battery, limited power and limited storage that makes the energy consumption. Data transport is a core function for Wireless Sensor Networks (WSNs) with different applications having varied requirements on the reliability and timeliness of data delivery. While node redundancy, inherent in WSNs, increases the fault tolerance, no guarantees on reliability levels can be assured. Furthermore, the frequent failures within WSNs impact the observed reliability over time and make it more challenging to achieve the desired reliability. Data transport is affecting by various attacks, such as delay attach, DoS Attack, Black hole attack, etc. This paper concentrates on the Delay attack and presents the detail study of recent techniques which were working on delay attack detection and prevention in WSN. This paper also provides the advantages and disadvantages of these techniques.

Index Terms— Data transport, WSN, Delay attack, reliability, DoS Attack, Sensor nodes, black hole attack.

1 Introduction

HIS document is a template for Microsoft Word versions 6.0 or Wireless Sensor Networks (WSNs) constitute a rapidly growing research area covering both a wide variety of devices and applications. Typical applications involve tracking or monitoring as (a) either statically as embedded sensors or (b) dynamically as mobile (semi) autonomous entities. Correspondingly, applications such as monitoring of traffic, disaster scenarios or target detection are seeing increased use of WSNs. Empirically the core function for a WSN is to collect data from the environment and transport it to a gateway node termed as sink. The general data collection and dissemination process involves the flow of the raw data from source nodes towards the sink.

Typically a WSN comprises of a large number of sensor nodes possessing limited processing and power capabilities, often communicating over unreliable and low bandwidth radio links. Consequently, this resource constrained environment is also subject to frequent node and communication failures. However, the utility of a WSN based application arises from delivering reliable services, necessitating the incorporation of fault tolerance techniques. A common approach to provide fault tolerance in WSNs is using node redundancy. However, this approach is not sufficient to fulfill the requirements of the application. Users are interested in detecting a targeted phenomenon (fire detection, tracking) with a certain quality, e.g., they may require no false negatives with or without tolerating false positives. Thus, the desired responsiveness, i.e., reliability and timeliness of data transport often varies for different applications. In extreme cases, there are applications that may require limited responsiveness such as habitat monitoring, and others that require high responsiveness such as military applications. Other intermediate responsiveness classes can be identified such as applications that do not require high delivery reliability but require delivery timeliness, i.e., if some data is lost the application performance will not degrade but data should reach within time bounds specified by the application.

Transport protocols are used to eliminate or mitigate congestion and reduce packet loss, to provide fairness in bandwidth allocation, and to guarantee end-to-end reliability. The transport protocol runs over the network layer protocol. It enables end-to-end message transmission, where messages are fragmented to chains of segments at senders and reassembled at receivers. The transport protocol usually provides the following functions: orderly transmission, flow control and congestion control, loss recovery, and possibly QoS guarantee such as timing requirement and fairness. In WSNs many new factors such as the convergent nature of upstream traffic and limited wireless bandwidth can cause congestion. The congestion influences normal data transmission and leads to packet loss. In addition, wireless channel introduces packet loss due to high bit-error rate, which not only affects reliability, but also wastes energy. As a result, two major problems that WSN transport protocols need to cope with are congestion and packet loss.

Attacks in Wireless Sensor Networks:

Black Hole Attack: Black hole attack occurs when an attacker captures and attacker reprograms a set of nodes in the network to block the packets which they receive instead of forwarding towards base station. Important Event information do not reach the base stations. In presence of black hole attack throughput becomes very less and end-to-end delay increases.

Gray Hole Attack: In gray hole attack, normal nodes work very unpleasant way which shows itself as a normal node and takes part in the transmission of packet from packets. These unpleasant nodes drop the selected packets and only transmits the left packets to the neighbor node.

Misdirection attack: In misdirection attack, malicious nodes misdirect packets to other destination. Here while sending packets some packets change its direction during transmission.

DoS attack: DoS attack is an attempt to make a machine or network resource unavailable to its intended users. A denial of service attack is characterized by an explicit attempt by attacker to prevent legitimate user of a service from using that service.

Delay Attack
In this type of attack, packets are not reached to destination node as per their specified time

2 Literature Survey

In this paper [1], a common security mechanism is proposed to mitigate pulse delay attack and node replication. This mechanism includes detection and then mitigation. By using this proposed approach the problem of pulse delay attack and node replication attack or clone attack can be detected and mitigated. This approach will make the wireless communication secure and reliable. This type of efforts can increase security of wireless sensor networks.

This paper [2], done a topological analysis of WSN in the presence of misdirection attack and presented an algorithm for the prediction of delay and throughput. It observed that WSN performs better for tree network topology as compared to mesh topology. In misdirection attack, the intruder misdirects the incoming packets to a node other than the intended node. Due to this attack, high end- to- end delay (sometimes infinite) is introduced in the network and performance of the network (i. e. throughput) is degraded.

This paper [3], presents a data forwarding scheme to defend jamming attack in WSN. The attack is defended at the cost of an affordable delay. The scheme considers a multilevel tier architecture based on clustering of nodes in each tier. Further the work identifies the parameters causing delay in presence of attack and analyses the impact of the parameter values in estimating delay. It claims that delay is affordable as it is independent of number of attacked-nodes rather it depends on number of tiers where attacked-node(s) belong.

This paper [4], introduces a security-oriented delay assignment algorithm for mitigating single and multi bit attacks. The algorithm enables a reduction of the correlation between the processed data and the consumed current by utilizing the data-dependent delays as a source of correlated noise. This is done while minimizing the area overhead, propagation time, and power. It show that for the same security level this new algorithm provides X2 and X6 more area efficiency, and X1.5 and X2.25 higher frequencies than a permuted path delay assignment and random embedding of delay elements.

This paper [5], propose an artificial neural network based energy-efficient and robust routing scheme for WSNs called ELDC. In this technique, the network is trained on huge data set containing almost all scenarios to make the network more reliable and adaptive to the environment. Additionally, it uses group based methodology to increase the life-span of the overall network, where groups may have different sizes. An artificial neural network provides an efficient threshold values for the selection of a group's chief node and a cluster head based on back propagation technique and allows intelligent, efficient, and robust group organization. Thus, this proposed technique is highly energy-efficient capable to increase sensor nodes' lifetime. Simulation results show that it outperforms LEACH protocol by 42%, and other state-of-the-art protocols by more than 30%.

This paper [6], describes a novel, simple, and effective method to thwart TDS attacks on SL. The proposed method works by augmenting the controller with a time-delay estimator to estimate any time delays. The modified controller controls the system under TDS attack. Also, the time-delay estimator will track time delays introduced by an adversary using a modified model reference control with an indirect supervisor and a modified least mean square minimization technique.

This paper [7], proposed a novel Cluster Based Intrusion Detection and Prevention Technique for Misdirection Attack. The network parameters calculated by the use of this technique shows considerable amount of improvement in throughput while introducing small amount of delay. The presence of misdirection attack affects entire performance of network especially throughput and End to end delay. The proposed cluster based intrusion detection and prevention technique is very effective to detect and prevent misdirection attack. Throughput has increased considerably by proposed method but it has introduced some delay.

This paper [8], developed and analyzed a novel hybrid delay- and loss-based congestion control algorithm, namely the DCCC algorithm. The proposed algorithm is able to i) maintain a bounded delay communication if the network conditions allows it; ii) prevent starvation when competing against loss-based flows. Introducing a price measure based on the interarrival time of the packets, we are able to provide a controller that automatically behaves as delay-based and loss-based protocol, based on the actual event that triggers the congestion. Moreover, because of the non-linear mapping between the experienced delay and the delay-based congestion signal, the DCCC algorithm avoids starvation when competing against loss-based flows.

This paper [9], propose two parametrized collaborative intrusion detection techniques and optimize their parameters for given scenarios using extensive simulations and multi objective evolutionary algorithms. Moreover, sample the whole search space to enable evaluation of evolution performance. It evaluates the influence of changes of the number of malicious nodes on the intrusion detection performance. The approach where choose from a set of non dominated solutions based on current WSN application, security and other requirements anytime after the optimization process can be easily adapted to practical applications. However, the optimization should be performed on a carefully configured simulator with an accurate model of target WSN. Both detection techniques can be easily combined into single IDS distinguishing selective forwarding and delay attacks.

In this paper [10] the aim of the paper is to form the game theoretic model of the jamming attack, to understand the different strategies of jamming game when jammer behaves in different ways. The paper also proposes the game theory based detection mechanism for all kind of jamming attacks. The proposed detection mechanism shows better energy consumption, throughput, and delay in different realistic situations of network (e.g. varying- amount of traffic and number of malicious nodes) as compared with existing optimal strategy solution.

Table 1: Survey table

Sr.no	Paper Title	Method Used	Advantages	Disadvantages
1	Detection and Mitigation of node Replication with pulse delay attacks in wireless sensor network	A common security mechanism is proposed to mitigate pulse delay attack and node replication.	It can increase security of wireless sensor networks and it will make secure and reliable wireless communication.	It is not energy efficient and cost efficient.
2	Misdirection attack in WSN: Topological analysis and an algorithm for delay and throughput prediction	It have done a topological analysis of WSN in the presence of misdirection attack and presented an algorithm for the prediction of delay and throughput.	It performs better for tree network topology as compared to mesh topology.	It degrades the performance of network.
3	Estimating delay in a data forwarding scheme for defending jamming attack in wireless sensor network	It presents a data forwarding scheme to defend jamming attack in WSN.	It is independent on the no of attack nodes and it is affordable.	It is not more realistic.
4	CPA Secured Data-Dependent Delay-Assignment Methodology	It introduces a security-oriented delay assignment algorithm for mitigating single and multi bit attacks.	It is efficient.	DOS attack is not detected.
5	ELDC: An Artificial Neural Network based Energy-Efficient and Robust Routing Scheme for Pollution Monitoring in WSNs	It proposes an artificial neural network based energy-efficient and robust routing scheme for WSNs called ELDC.	It is highly energy-efficient	Reliability is not consider

3 Proposed Approach

For input transporting data developed a data gathering protocol named as Broadcasting Combined with Multi-NACK/ACK (BCMN/A)and used for time constrained data collection. Also, secure data by making use of proposed delay attack detection technique.

In contribution, the system detects the delay attack and make the system more secure. Here in proposed network selection of Cluster Head is perfumed based on Energy of the node as well as the distance of the node from Base Station to increase the efficiency. This system makes use of ECC algorithm to provide security while data transportation. Here data is sent encrypted format, so that if any attack is occurred the attacker can't able to read the data. After data transfer, the cluster head checks that data is received from all the CM within an allocated time. If the data from node (CM) is not received to the CH within allocated time period then CH broadcast that particular CM ID in a network. Still, if the data is not received from that CM then it is detected as a delay attacker and discarded that CM from the network.

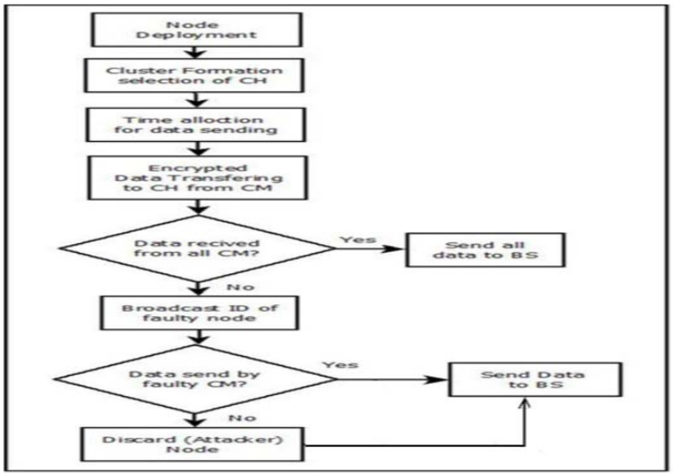
Node Deployment
Cluster Formation selection of CH
Time alloction for data sending
Encrypted Data Transfering to CH from CM
Data recived from all CM?
Yes
Send all data to BS
No
Broadcast ID of faulty node
Data send by faulty CM?
Yes
Send Data to BS
No
Discard (Attacker) Node

Figure 1: System Architecture

4 Conclusion and Future Scope

In this survey, we have studied different attacks like delay black hole attack, gray hole attack , misdirection attack and DOS attack in WSN. Wireless Sensor Networks are mainly used in monitoring and control. Moreover WSN are mainly used for specific application. From this survey we conclude that, the delay attack is very harmful for such application, which need to be solved. This paper also provides the comparative analysis of some recent techniques for detection and prevention of delay attack.

References

[1] Umrao, Sachin, Deeksha Verma, and Arun Kumar Tripathi. "Detection and Mitigation of node Replication with pulse delay attacks in wireless sensor network." Innovation and Technology in Education (MITE), 2013 IEEE International Conference in MOOC. IEEE, 2013.

[2] Sachan, Roshan Singh, et al. "Misdirection attack in WSN: Topological analysis and an algorithm for delay and throughput prediction." Intelligent Systems and Control (ISCO), 2013 7th International Conference on. IEEE, 2013.

[3] Ghosal, Amrita, et al. "Estimating delay in a data forwarding scheme for defending jamming attack in wireless sensor network." Next Generation Mobile Applications, Services and Technologies, 2009. NGMAST'09. Third International Conference on. IEEE, 2009.

[4] Levi, Itamar, Alexander Fish, and Osnat Keren. "CPA Secured Data-Dependent Delay-Assignment Methodology." IEEE Transactions on Very Large Scale Integration (VLSI) Systems (2016).

[5] Mehmood, Amjad, et al. "ELDC: An Artificial Neural Network based Energy-Efficient and Robust Routing Scheme for Pollution Monitoring in WSNs." IEEE Transactions on Emerging Topics in Computing (2017).

[6] Sargolzaei, Arman, Kang K. Yen, and Mohamed N. Abdelghani. "Preventing time-delay switch attack on load frequency control in distributed power systems." IEEE Transactions on Smart Grid 7.2 (2016): 1176-1185.

[7] Sachan, Roshan Singh, et al. "A cluster based intrusion detection and prevention technique for misdirection attack inside WSN." Communications and Signal Processing (ICCSP), 2013 International Conference on. IEEE, 2013.

[8] D'Aronco, Stefano, et al. "Improved Utility-Based Congestion Control for Delay-Constrained Communication." IEEE/ACM Transactions on Networking (2016).

[9] Stehlik, Martin, Vashek Matyas, and Andriy Stetsko. "Towards better selective forwarding and delay attacks detection in wireless sensor networks." Networking, Sensing, and Control (ICNSC), 2016 IEEE 13th International Conference on. IEEE, 2016.

[10] Babar, Sachin D., Neeli R. Prasad, and Ramjee Prasad. "Game theoretic modelling of WSN jamming attack and detection mechanism." Wireless Personal Multimedia Communications (WPMC), 2013 16th International Symposium on. IEEE, 2013).