International Journal of Engineering & Technology, 7 (2.24) (2018) 489-491

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Co-operative Detection for Malicious Nodes in Under-Attack WSN

Shweta Ranjan Vikas [1], B. Priyalakshmi [2], Nikita Gautam [3], Sairam Potti [4]

[1,3,4]Student, [2]Asst.Professor,
Telecommunication Engineering, SRM IST, Chennai, Tamilnadu, India
**Corresponding Author Email: shwetaranjan.21@gmail.com*

Abstract

The network security must be taken into consideration in wireless sensor networks. In our project, we take sensor node data falsification (SNDF) attack using malicious nodes and co-operative detection is used. Fusioncentre collects information from the nodes created in a cluster environment and makes a global decision. The protocol used here is Ad-hoc-on demand distance vector[5] (AODV) and the performance analysis is done using parameters such as throughput and End-to-end delay. The stimulation is done in NS2 using network animator and graphical results are taken.The throughput will be increased compared to the existing system whereas End-to-End delay will be decreased.

Keywords: *Fusion Center, Sensor Node Data Falsification, Wireless Sensor Networks, Ad-Hoc On- Demand Distance Vector Protocol.*

1. Introduction

In wireless sensor networks, the security threats have become a major issue today. To overcome security threats many detection techniques have been introduced. In our project, we use centralized detection technique. It is conveyed over a field and different SNs report their handled perceptions to combination focus. It at that point consolidates them to shape a worldwide choice. Sadly these small gadgets experience the ill effects of compelled bandwidth and onboard control. Moreover, topographically dispersed nature of these hubs makes them helpless against different kinds of assaults. Thus embeddings security in WSN has turned into a testing assignment.
Wireless security has two types of goals. They are primary and secondary. Confidentiality, Availability, Integrity and Authentication are some of the primary goals. Some of the secondary goals include Self-Organization, Secure localization, Time synchronization and Resilience to attacks. Various types of attacks bestowed upon wireless sensor networks are jamming, spoofing, wormhole, Sybil, sink hole, sensor node data falsification attack etc.,
A different system of disseminated recognition under attack−free WSNs has been broadly considered in [4]-[11], to give some examples. While references [4]-[8] think about circulated identification by expecting boundless transmission capacity/assets in WSNs, the creators of [9]-[11] unwind this presumption by considering appropriated recognition over data transfer capacity obliged/vitality compelled WSNs. In any case, these methodologies are powerless against security dangers as a portion of the SNs answering to the FC might be traded off. Subsequently, the FC isn't vigorous against such assaults and its identification execution will be corrupted. In this work, we additionally consider the sensor hub information distortion (SNDF) assault in which the traded off SNs send wrong neighbourhood choice reports to the FC.
In this project,three different cluster environments is formed. Thirty-three nodes are randomly distributed in above three clusters.

2. Proposed System

a. Cooperative detection

To protect data reliability in wireless sensor networks, we propose cooperative-based falsification detection and an isolation mechanism for the malicious nodes that are detected.
In our proposed mechanism, we define the following nodes:
• Proper node: a node at the initial configuration on the network that can transmit both the original packet and forward other packets.
• Cooperative node: a proper node that is also a common neighbour node of two successive nodes in a route.
• Monitoring node: a new-entry node and a re-entry node to a network. It can forward a packet but is not permitted to transmit the original packet.
• Malicious node: a node with a stolen shared key with which it can falsify packets and mask falsification from other malicious nodes.
• Isolation node: a node through which falsification is detected by proper nodes
To create an environment, where a cluster of nodes is formed. Then assign a cluster head to each cluster. The cluster head is present at the centre which communicates with all the other nodes as well as the FC.
Below is the figure which shows cluster formation and also FC.

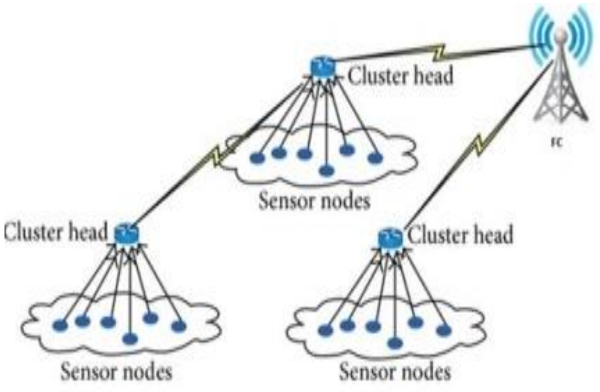


Fig. 1: Cluster Formation

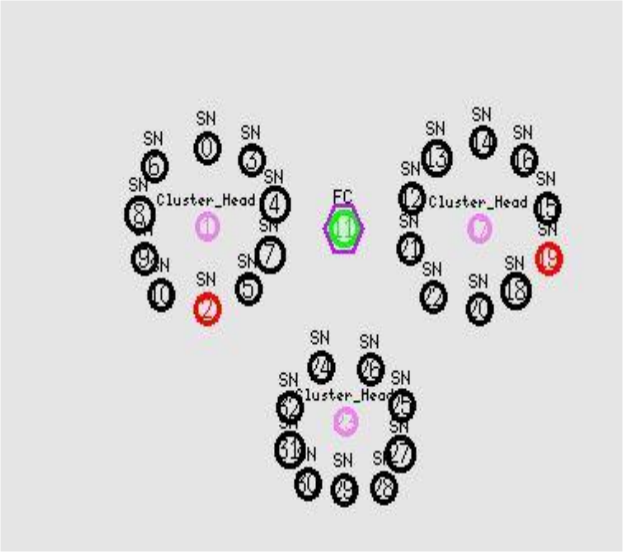
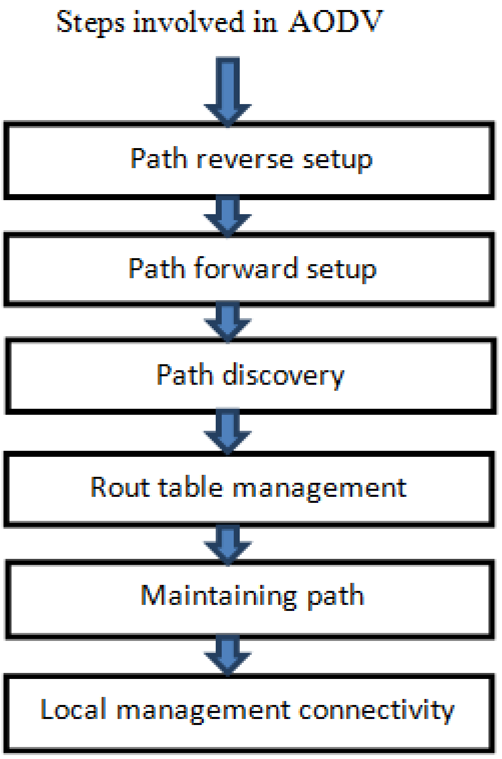


Fig. 2: Attack Formation

b. AODV Protocol

There are three types of protocol. Proactive, reactive and hybrid. Reactive protocol because it saves network bandwidth and also battery life of nodes. One of the types of the reactive protocol is the Ad hoc on demand distance vector protocol (AODV)[5].
Ad-hoc on-demandvector[5] is a routing protocol for an ad-hoc mobile network with huge number mobile nodes.
The algorithm creates routes between nodes only when the source node asks for it, giving the network the willingness to allow nodes to enter and leave the network
An ad hoc routing protocol controls how nodes decide which way to route packets between computing devices in a ad hoc network.
Familiarity of topology with the networks is not considered in adhoc networks. The discovery should be made on its own and nodes should find their own route for broadcasting to their neighbors.



Advantages of AODV:
1. Scaled to a large population of nodes.
2. The broadcast reduction.
3. Memory requirements and needless duplications have been reduced.
4. Maintaining of Loop-free routes using destination sequence numbers.
5. Node store is route that is needed.

c. Sensor node data falsification attack

Interpretation Data Falsification (IDF) Attack: In this type of attack the attacker falsely senses the data and sends to its neighbors. In information blending phase, the attacker nodes correctly update their estimated value and send it to their neighbors. This attack is difficult to differentiate from other nodes , but easy to implement.
Step by step in Data Falsification (SDF) Attack: The attack takes place both in the beginning and also in each of the steps making it a step by step procedure. It can harm the network for a longer period of time.
Unpredictable Data Falsification (UDF) Attack: The attacker can attack at any period of time regardless of the transmission going on. This type of attack can be concealed very easily hence making is very difficult to detect.

d. Performance analysis

Stimulation helps us to analyze and evaluate the performance and behaviour of the network before implementing it in real life application.
In this paper, some performance metric for evaluating routing protocol has been considered. We calculate packet delivery ratio, throughput and end-to-end delay. The test analysis will be printed in graphical format.
Our simulation is done in NS2 using tool command language. The network animator window shows the attack and sense of nodes.

Table 1: Parameters

Nodes	33
Attacks	2
Antenna	Omnidirectional
Stop Time	40 Sec
Channel	Wireless
Mac	Mac/802_11
Detection	Co-Operative

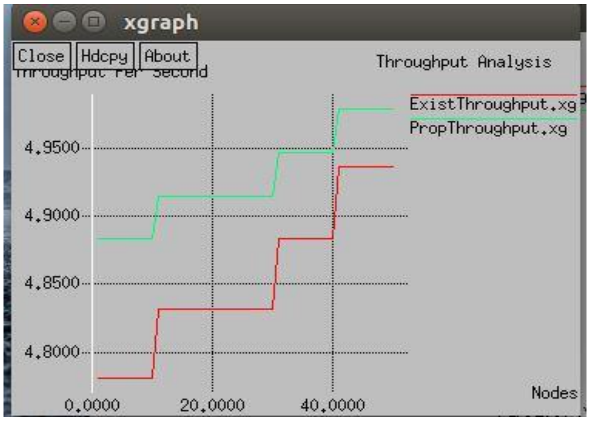


Fig. 3: Throughput Analysis

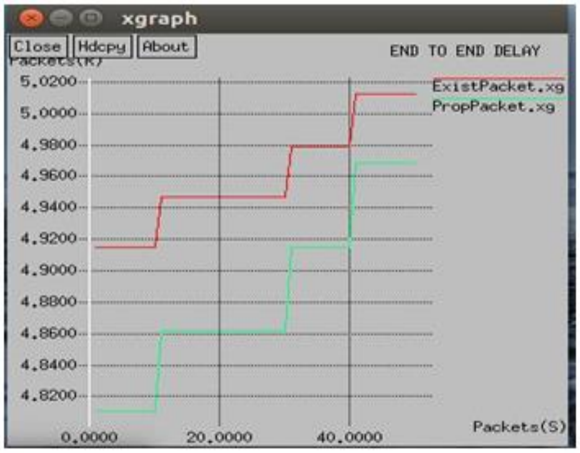


Fig. 4: End to End Analysis

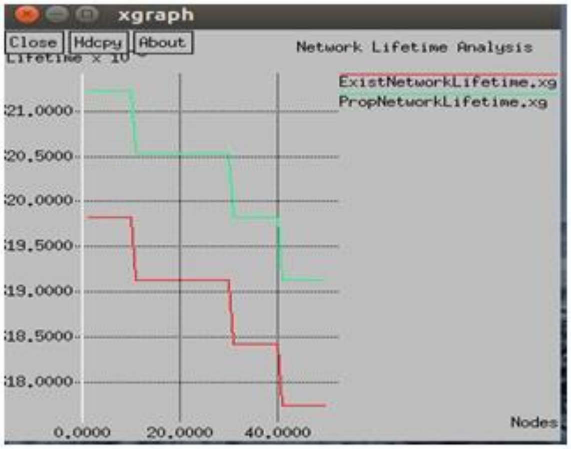


Fig. 5: Network Life Time Analysis

Formulae Used

The primary method of doing calculations with Tcl's **expr** command. The below formula is a tcl command which in general is used for analysis purpose in ns2. Our paper uses the same formula/

setv[expr”$a$op$b”]

Using above throughput, end-to-end delay, network lifetime analysis can be calculated.

3. Conclusion

Our paper describes the node formation and attack on the nodes. Then using co-operative detection technique, throughput, end-to-end delay, network lifetime analysis have been calculated. The graphical results are shown above.

4. Future Work

To protect the reliability of wireless sensor networks without a secure key, we propose a mechanism that detects malicious nodes by the cooperation of proper nodes and logically isolate the detected, malicious nodes from wireless sensor networks.

References

[1] VP.Illiano, and EC.Lupu: Detecting Malicious Data Injections in Wireless Sensor Networks: A Survey, ACM Comput.Surv., Vol. 48, No. 2, Article 24 (2004).

[2] S. Prasanna, and S. Rao: An Overview of Wireless Sensor Networks, IJSCE, Vol. 2, Issue. 2, pp. 538-540 (2012).

[3] H. Chan, and A. Perrig: Security and Privacy in Sensor Networks, IEEE C.S., Vol. 36, Issue. 10, pp. 103-105 (2003).

[4] X.Du and H.Chen: SECURITY IN WIRELESS SENSOR NETWORKS, IEEE wirel. commun., pp. 60-66 (2008).

[5] KamarularifinAbdjalil, Zaid Ahmad et.al, "Securing Routing Table update in AODV Routing Protocol", 2011 IEEE conference on open system.

[6] Y. Cho, G. Qu, and Y. Wu: Insider Threats against Trust Mechanism with Watchdog and Defending Approaches in Wireless Sensor Networks,S!uP, pp. 134-141 (2012).

[7] A.Aikebaier, M. Jibiki, Y. Teranishi, and N. Nishinaga: Proposal and Evaluation of a Cooperative Malicious Node Isolation, IEICE Technical Report IA, 2013-73, pp. 31-36 (2014)

[8] JaydipSen: A Survey on Wireless Sensor Network Security, IJCNIS, Vol. 1, No. 2, pp. 55-78 (2009).

[9] A. Perrig, R. Szewczyk, J. D. Tygar, V. Wen, and D. E. Culler: SPINS: Security protocols for sensor networks, Wire l. Netw., Vol. 8, Issue. 5, pp. 521-534, (2002).

[10] A. Ailixier, J. Masahiro, T. Yuuichi, and N. Nozomu: A Proposal of Cooperative Malicious Behavior Node Isolation Mechanism for Wireless Sensor, IPSJSIGTechnical Reports, Vol. 2013-EIP-61, No. 9, pp. 1-7 (2013).

[11] T. Karygiannis and L. Owens, “Wireless network security,” NIST special publication, 2002.