Volume 4, Issue 7, July 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Misdirection Attack in WSN Due to Selfish Nodes; Detection and Suppression using Longer Path Protocol

Juby Joseph
Department of CSE
Mangalam College of Engineering
Ettumanoor, Kerala, India

Vinodh P Vijayan
Department of CSE
Mangalam College of Engineering
Ettumanoor, Kerala, India

Abstract- Wireless Sensor Network (WSN) applications are extended to fields like consumer, industrial and defense sectors. Thus WSNs are attacked easily by different kinds of attacks out of which misdirection attacks are not easy to detect and defend.Misdirection attacks are a type of Denial of Service (DoS) attacks. Herethe attacker misleads the content packet to a different destination rather than the actual destination.Due to this situation, end-to-end delay of the network system will be randomly increases (sometimes upto infinity) which results in degradation of overall network performance. Misdirection attack due to the presence of selfish nodes will lead to the decreased efficiency and packet delivery. Some node behaves unexpected way and not forwards the packets and messages to the intended node.This paper proposed a new idea of longer path insertion for message transfer which is capable of suppressing the selfish behavior. The delay-throughput prediction algorithm is used for finding out the delay and throughput during packet delivery.It is expected that the throughput of the system will be improved through new protocol implementation.

Keywords-Misdirection attack, End-to-end delay, Throughput improvement, Longer path protocol, Selfish nodes.

I. INTRODUCTION

Wireless sensor nodes are deployed in remote sections, where resources for power systems are limited. Different applications of WSN include environment monitoring, military surveillance, etc. In some cases the confidential data is travelling from a source to destination without any security over the medium. Hence, one of the important problem of WSN is that it will be easily attacked by Denial-of-Service (DoS) attacks, which results in loss of actual information and thereby causes large energy expenditure. Therefore, ensuring the security of the links is important in designing a sensor network. In misdirection attack the intruder, directs the packet from its sub nodes to other distant nodes, but not necessarily to its super parent node. This produces long delay in packet delivery and decreases the throughput of the network. Misdirection attack is an attack occur in network layer with packet transmission loss occur between routers.

In ad hoc networks, wireless nodes depend on each other to transmit data over multi-hops by forwarding packets. A selfish node may try not to forward packets for other nodes to save its own resource but still use the network to send and receive data. Such a selfish behavior can adversely affect the network performance. Most existing work took observation, reputation and token based mechanisms. However observation based mechanism suffers from mobility and collusion; reputation and token based mechanisms suffer from system complexity and efficiency. The Longer path protocol (LP) protocol is capable of suppressing selfish behavior. Basing on the fact that the selfish nodes still want to receive and send packets, if a node cannot determine whether a packet is destined for it or not, it won't be able to drop the packet. With specific modifications, LP achieves the design target. It is robust and efficient. To solve the problem of selfish behaviors, it is important to handle the following conditions effectively: It must perform under various network conditions, The system computation complexity must be less ,Should not consider the isolated nodes and finally help all the nodes in packet transmission. Since the existing schemes have different built-in problems ,it is important to design an elegant scheme to suppress the selfish behavior.

- ***Wireless Sensor Networks(WSN)***

Wireless sensor networks are group of sensor nodes deployed in physical environment scenarios. These sensor nodes are easily affected by various attacks .So in order to detect the attacks intrusion detection system(IDS) are used . WSNs are ideal candidates for monitoring environments in a wide variety of applications such as military surveillance and forest fire monitor, animal identification etc,. In wireless environment the sensor nodes are defenseless or vulnerable against attacks.WSN platforms generally have limited processing capability and memory. The design of WSN devices usually favors decreased cost over increased capabilities. The basic characteristics of sensor networks make them vulnerable to DoS attacks. Since they are shared by all devices in the network, it is not easy to keep them stable. Any adversary in radio range can overhear traffic, transmit spurious data, or jam the network.

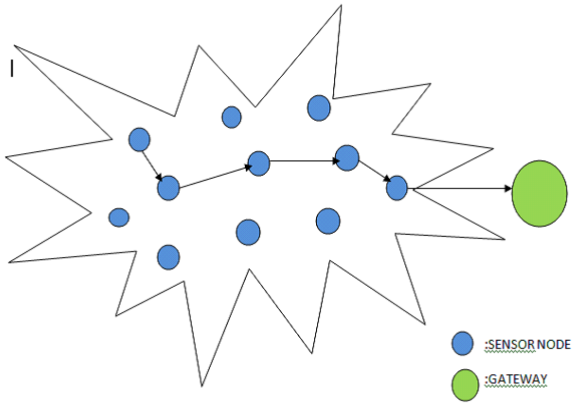

Fig 1: Wireless Sensor Networks

II. RELATED WORKS

Misdirection attacks very negatively affect the overall system of ad hoc networks. Hence it is important to perform some analysis and experiments to improve the performance through throughput calculation. There are certain works in which techniques introduced for predicting the delay and throughput [1] of the network. But these techniques failed to solve the problem of misdirection attack suppression.The use of the results of hashing data packets as session keys to encrypt same data packets, does not require any additional[2] energy expenses. But it is not able to implement on hardware platforms. A system of Immediate authentication of each packet when it is received, without disrupting the efficient propagation[3] mechanisms also a good technique.But There will be interference between the code dissemination packages since the neighbor relationships are simulated, which cause a variation in performance. Application of one-dimensional 3-neighborhood reversible cellular automata for securing WSNs is the another practice used in this area [4]. High energy expenditure and less reliability are its disadvantages. A Secure multi-hop routing in WSNs against intruders exploiting the replay of routing information and Trust management idea for reliable route selection also can be used [7].But it is not good in malicious node detection.

III. SYSTEM DEFINITION

Misdirection attack is the most popular DOS attack in WSNs. A malicious node could deny a valid route to a particular node thereby denying service to the destination. Misdirection attack can be performed in different ways.

A. Packets forwarded to a node close to the actual destination

This kind of misdirection attack is less intense, because packets reach to the destination but from a different route which further produces long delay, thus decreasing throughput of network (bit transfer per second).

B. Packets forwarded to a node at a large distance from the actual destination

This kind of misdirection attack is very harmful because all packets are forwarded to a node far away, preventing them to reach the destination so packets will not reach destination.[6] Due to the attack the delay becomes infinite and further results in zero throughput.

C. Intermediate node become selfish node

Here a node in the transmission path will behave selfishly and not forward the message packet to the actual destination. Thus here also the delay will be higher and throughput will decrease. The delay-throughput prediction algorithm is capable of finding out the parameters during the misdirection attack conditions.

D. Delay-Throughput prediction algorithm

If packets forward to a node, close to the destination
predicted delay=Normal delay + change in delay
throughput predicted=Normal throughput-change in throughput
Otherwise
predicted delay=Infinity
predicted throughput=0

The selfish node suppression can be effectively obtained through the implementation of Longer Path(LP) protocol

(1)Is LP Protocol suitable for Selfish Behavior Suppression?

It's very important that the real destination of a packet is unknown to intermediate nodes. When a node receives a packet, it cannot open the packet and even doesn't know whether the real destination is that node or not. The packet knows whether it is the real destination only after it is forwarded and then it gets the key for reading the content of the packet.

In LP protocol it needs the last node in the network must be capable of send back an acknowledgement and key to the previous node. But the last node may behave selfishly for saving its time and energy.

Initially the message(acknowledgement +key)is very small and the energy expenditure on that message is negligible .Another point is that if the last node is selfish ,the probability of dropping the packet get decreased. So with the help of LP protocol, the last node in the transmission can drop the message selfishly.

It is important to select the best last node for longer path construction .So, it is achieved by certain observation mechanisms; only for last nodes and not for all nodes. In LP, the destination node must either forward an acknowledgement to the source node or forward the packet to the next node. So when a node transmit a packet and not get any reply from the next, then that next node is identifies as a selfish node.

IV. SYSTEM DESIGN

The selfish behavior can be a significant problem to the overall system performance. When there are 10% selfish nodes, the throughput of network can be degraded to about half of the overall performance; and when half of the nodes in the network are selfish, the throughput will be very small which results in incapability of network in packet transmission. Thus, a small number of selfish nodes may result in negative impact of the network. More importantly, the selfish nodes will try to make negative impacts on the remaining nodes of the network for reliable and secure packet transmission.ie, The malicious nodes in the network try to destroy the other nodes and not for their own resources. For example, Jellyfish attack is a type of attack in which the attackers disturb data transmission by dropping, reordering and delaying packets.

A) Longer Path(LP) protocol

The LP protocol encrypts packets, makes the real destination of a packet not equal to the last destination of route path, and gives nodes acknowledgements from its next hop if the node
is the real destination.

Initially, the message packet will be encrypted using any basic encryption standard .If a node in the network wants to see the packet, it needs the key first. So, when a node has a packet to send, it must generate a random key for encrypt the message and generally uses a symmetric encryption algorithm as Data Encryption Standard(DES).So in the next levels the message will be the cipher of DES with key K.DES encryption can be performed very fast and have the lowest cost.

Next, a longer path route will be discovered for packet transmission. LP protocol needs to find not only the path from actual sender to receiver but also the longer path. So, then message obtained initially will be send through the longer path. But before forwarding, the user must add an information in the packet that whether the destination of that packet is its previous node. Hence a node will identify whether that packet is destined to it and is not received from the next node. Thus it can forward the packet to the next node.

In the next step, when a node gets a packet ,it pull out the actual information from the encrypted version and identifies whether the packet's destination is its previous node .If happen so, then send back an acknowledgement. Otherwise the packet will be moved to the next nodes.

If a longer path cannot be found, the source node also prepares information for each node: whether this packet's real destination is the node's previous node and if the destination is the node itself, then the key K to open the packet.

B) Levels of Implementation

The system scenario includes different levels for implementation.

(1)Routing Information Table Creation

Generally the WSN environment includes number of sensor nodes for communication and exchange of message or information. When sending or receiving of information through a particular node taking place, a routing table must be generated so as to achieve the reliable transport of message. So, each of the node must have a routing information table which have the information's like node-id, source node, destination node, packet id, number of hops etc..Based on the table information, one node can undoubtedly determine its next destination and also identify the node from which it receives the packet.

(2)Forwarding and Dropping Ratio

The detection of forwarding and dropping ratio will help to easily identify the amount of data transmitted and received. Forwarding ratio is the ratio of total packets generated to the total packet sent. whereas Dropping ratio is the ratio of total packets sent to the total packet lost.

(3)Attacking node(Selfish node)Detection

One node which is capable of causing attack is treated as an attacker node. Here a threshold value will be generated based on the predefined values. When the data rate of a particular node is higher than the threshold value obtained, then that node will be treated as an attacker node. Based on the packet transmission at each time ,a matrix will be created which identifies the position of packets at which node.

(4) LP Protocol Implementation

Based on the information obtained the Longer Path(LP) Protocol is implemented. It includes different steps to obtain a one more node through a long path other than the actual path through the current destination.

V. PERFORMANCE EVALUATION

A setup for conducting the experiment have arranged with ONE(Opportunistic Network Environment) simulator with a simulation time of 30 minutes. The network architecture includes 50 nodes and 5 routers for the initial system development.

TABLE I: OTHER PARAMETERS OF EXPERIMENT

Parameter	*Value*
Packet Inter- Arrival Time (sec)	Constant (1)
Packet Size (bits)	Constant (1024)
CSMA/CA Parameters	Default
Sensing duration (sec)	0.1
Physical Layer Parameters	Default

The results and graphs are obtained for packet delivery probability and system overhead.

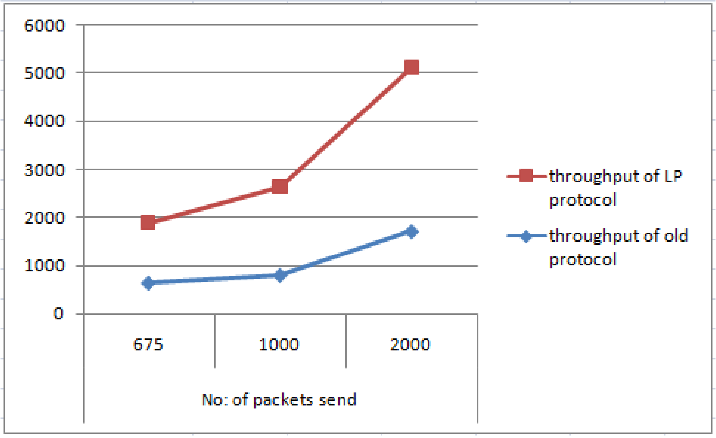

Fig 2: Packet Delivery Probability

Packet delivery probability is a positive factor where the throughput is tremendously increased than the old protocol.

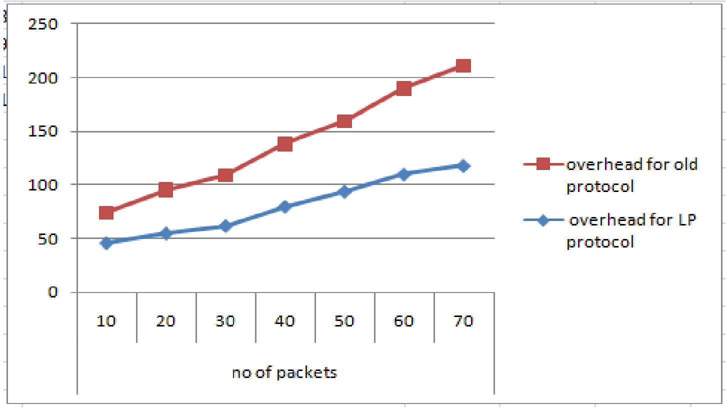

Fig 3: System Overhead

System overhead is a positive factor where the overhead value is reduced for LP protocol.

VI. CONCLUSION

Misdirection attack adversely affects the network performance. In most cases the throughput of the system decreases and delay increases. And thus overall system performance will get affected. The proposed scenario of Longer Path protocol is capable of effectively reduce the selfish nature of a node in the network .This goal is achieved through perfect routing and encryption standards. Simulations are supervised to evaluate the LP performance from different means. The results show that LP achieves higher grades of performance and capable of giving good result in different conditions.

VII. FUTURE SCOPE

Since encryption standards are used for packet transfer it is highly time consuming. Thus future work is done for reducing the time delay.

ACKNOWLEDGEMENT

I am very thankful to all those people, who guided and supported me. Without their valuable guidance and support, this task was not possible.

REFERENCES

[1] Roshan Singh Sachan,MohammadWazid, D.P. Singh, Avita Kata and R.H. Goudar5, "*Misdirection Attack in WSN: Topological Analysis and an Algorithm for Delay and Throughput Prediction"* ,january 14,2013.

[2] Hailun Tan, DiethelmOstry, John Zic, Sanjay Jha, "*A Confidential and DoS-Resistant Multi-hop Code Dissemination Protocol for Wireless Sensor Networks*", ACM WiSec'09, March 16-18,2009.

[3] An Liu, Y oung-Hyun Oh, Peng Ning, "*Secure and DoSResistant Code Dissemination in Wireless Sensor Networks Using Seluge*", ACM International Conference on Information Processing in Sensor Networks 2008.

[4] SomanathTripathy, Sukumar Nandi, "*Defense against outside attacks in wireless sensor networks*", Elsevier Computer Communications, Volume 31, Issue 4, 5 March 2008.

[5] Guoxing Zhan, WeisongShil, Julia Deng, "*TARF: A Trust Aware Routing Framework for Wireless Sensor Networks*", EWSN 2010, LNCS 5970, pp. 65-80, 2010.

[6] M. Y. Abdullah, Hua Gui Wei, N. Alsharabi, "*Wireless sensor networks misdirection attacker challenges and solutions*", IEEE International Conference on Information and Automation, 2008.

[7] PoWahYau, Shenglan Hu, Chris 1. Mithell, "*Malicious attacks on ad hoc network routing protocols*", International Journal of Computer Research Vol 15 Issue 1,2007.