International Journal of Contemporary Research in Computer Science and Technology (IJCRCST) ISSN: 2395-5325
Volume 3, Special Issue 1 (February '2017)
Special Issue on 1st National Conference on Advanced Computing and Communication Technologies,
Conference held at Siri PSG Arts and Science College for Women, Sankari,Tamilnadu,India.

A HYBRID MODEL OF DEFENSE TECHNIQUES AGAINST BASE STATION JAMMING ATTACK IN WIRELESS SENSOR NETWORKS

M.Malathi,
Ph.D Research scholar,
Periyar University,
Salem,Tamilnadu,India.

Dr. A.SenthilKumar,
Assistant Professor,
Department of Computer Science,
Arignar Anna Government Arts College,
Namakkal, Tamilnadu,India.

Abstract: Wireless sensor networks (WSNs) are highly susceptible to jamming attacks due to their resource limitations .In WSN architecture, the Base station (BS) is a single point of failure, because it collects tasks. so BSs are main targets of the jamming attack. For mitigating the effects of BS jamming attack .we propose a hybrid model of defense, which combines 3 defense techniques. The first technique is BS replication, so in a jamming condition, there may be some unjammed replicated BSs for providing service to the network. The second technique is the evasion of BS from jammed is multipath routing for providing alternative paths for communication with BS in case of jamming of one or more paths. Through simulation .We show the effects of the hybrid model of defense on the communication traffic throughput of WSNs

Keywords: Wireless sensor networks, BS jamming attack, Multipath Routing

I.INTRODUCTION

The development of wireless sensor networks was originally motivated by military applications such as battle field monitoring. wireless sensor networks are now used in many industrial and civilian application areas, including machine health monitoring, environment and habitat monitoring, indoor sensor networks with sensor enabled user interfaces, home automation, and traffic control. As the applications of WSNs are increasing, providing security and trustworthiness is an important issue. In WSN sensor nodes have limited resources such as energy, computation power and storage available. The broadcast nature of communication in WSN significantly increases the capabilities of adversary to initiate Denial of service attacks. In a DoS attack, an adversary can deny to follow medium access protocol. In this manner it can continuously transmit on the wireless channel and prevent the legitimate user to perform MAC operations or introduce packet collision that force repeated backoffs, or even jam transmission.

Jamming attacks are representative energy consumption DoS attacks in WSN. Jamming is a well DoS attack, which interfaces with radio frequencies used by sensor nodes for communication. Anti-Jamming techniques such as spread-spectrum and lower duty cycle are not widely applicable for low cost sensor networks.

The Base station (BS) aggregates sensor readings and conducts command and control tasks. So it is a central point of failure and is an attractive target for jamming attack, because failing of it can render the whole WSN out-of-service during attack. In two defense strategies channel suffing and spatial retreats are used to evade a MAC/PHY layer jamming attack. In channel surfing, changing channels at the data link layer is more expensive, because it requires synchronization between both parties, which takes additional time. In spatial retreat, there is the evasion overhead in terms of energy and time consumed in movement and network reconfiguration, which can increase the effect if not carefully controlled. Mobile jamming attack is represented with multi-dataflow topologies scheme, the BS can receive messages from the affected area contionuously and the affected sensor nodes do not need to re-route under the mobile jamming attack.more than one topology causes more over head and lower connectivity in WSN. The authors have proposed two defense strategies secure multipath routing to multiple destination BSs and anti-traffic analysis strategies to disguise the location of BS.If multipath routing is not controlled carefully,communication cost can increase drastically.Anti-traffic strategies are also not very effective, because a lot of computational power requires for disguising the location of BS from eavesdroppers, which is not feasible in a resource limited WSN. This information is used to avoid route,which goes through this jammed region.These

jammed sensor nodes turn themselves into sleeping mode,so that they can outlast the energy of jammers.But the jammers can outlast the energy of jammers.But the jammers can detect no communication by these jammed nodes, and can turn themselves into lower duty cycle. This frame work combines BS replication and evasion defense techniques to mitigate the effect of jamming attacks.This framework,with moderate replication, performs better than other strategies,if the jamming attack is low to medium in strength.

A hybrid model of defense for mitigating BS jamming attacks in WSNs.The hybrid model is a combination of three defence techniques.the first technique is BS replication so in a jamming condition, there may be some unjammed replicated BSs,which can provide service to the network. The second technique is the evasion of **B**S from jammed location to any unjammed location,so in case of jamming attack on BS,it can physically move to any unjammed location,and reconfigure itself with the sensor nodes at that location. The third defence technique is multipath routing,so there may be some alternate paths available for communication with Bs in case of jamming one or more paths by jammers.In this work DYMO routing protocol to support multiple path data delivery. Our network framework and jamming attack model. We describe multipath extension of DYMO routing protocol .

II.PROBLEM OVERVIEW

A Jamming attack can be launched in data-link layer or physical layer. Link layer jamming attacks disturb the communication between sensor nodes around the jammer. physical layer jamming attacks. let the radios frequency interfere with the open wireless environment. the prime target for jamming attack because of their importance in aggregating sensor readings, and for playing role in protocols. A Hybrid model of defense against BS jamming attacking WSNs. The hybrid model contains a combination of three defense techniques.

Bs Replication: Our first defense technique is BS replication.There should be multiple replicated BS in WSN, so that in case of a jamming attack, if one or more BSs are not jammed. The WSN can continue delivering data for a longer time during such a jamming attack.When jammed BSs unjammed, they may request for the sensor readings from unjammed BSs. Figure 1 shows a WSN which consists of 5 BSs and 3 mobile jammers. Out of 3 jammers, 2 jammers successfully jam 2 replicated Bs. 3 BSs are not jammed and these can serve the whole WSN.

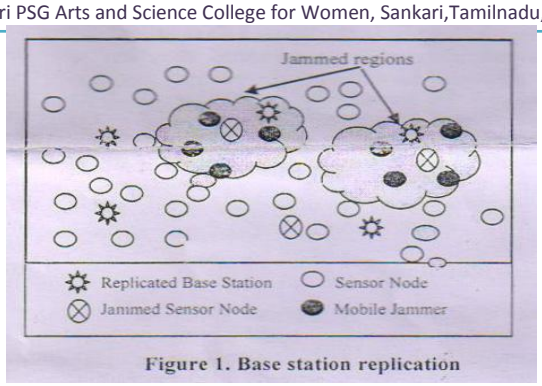

Figure 1. Base station replication

Bs Evasion: our second defense technique is BS evasion from jammed location to unjammed location.The BS should be mobile,so that in case of a jamming attack, it can physically move to any unjammed location. The hybrid model, replicated BSs change their physical location pro-actively with a pre-determined off-line schedule,so that more than one BS cannot collide by reaching the same location at the same time. Figure 2 shows a WSN consisting of a BS and 3 mobile jammers, one of which successfully jams a BS. But BS is mobile so it physically moves from jammed location to any unjammed location and again starts communication with sensor nodes.

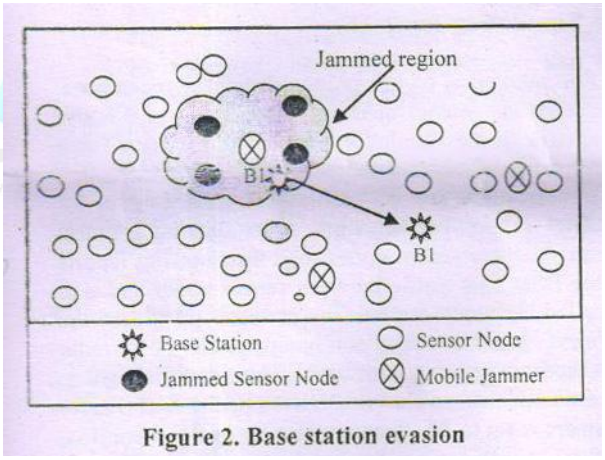

Figure 2. Base station evasion

III.MULTIPATH ROUTING

Our third defense technique is multipath routing. According to this technique, there should be multiple paths between sensor nodes and BS .so that in case of jamming attack if atleast one path between sensor node and BS is not jammed, the BS can get sensor readings through this path and the sensor network can continue working. Through multipath routing, traffic dispersion can be used to prevent eavesdropping, to do load balancing or to minimize the energy consumption by nodes. Traffic dispersion means that for a same source destination pair, communication simultaneously uses different paths instead of a single one. Figure 3 shows a WSN consisting of 5 BSs and 3 mobile jammers, one of which successfully jams a BS. There are two paths from sensor node under path p2 is jammed, sensor

readings are delivered by path p1. Thus there is no effect of jamming on unjammed BSs for reading the sensor information from unjammed sensor nodes.

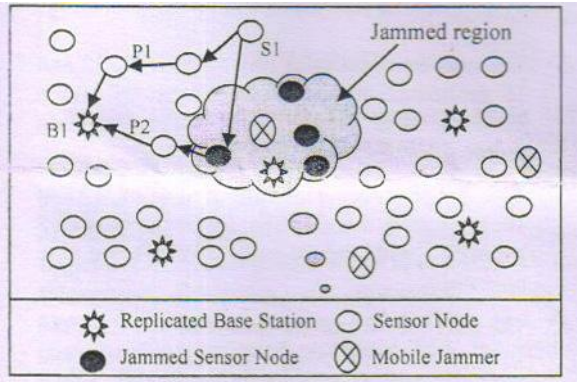

Figure 3. Multipath routing

IV. NETWORK FRAMEWORK AND ATTACK MODEL

Our WSN is organized in a tree – like structure, where BS works as a root node of the tree. Sensor nodes sense around and report the sensing result to the BS.sensing results contain the normal sensing data or alarm event messages. The sensor nodes under the jammed area are called jammed sensor nodes.These jammed sensor nodes cannot transmit data to the BS. According to a pro-active defense strategy,the BS roam among collection points using a pseudo-random schedule,pre-loaded off-line.It may be possible that the unjammed BS have to change location.while jammed BS may remain at their location.

Jamming Attack Model

1. An attacker can compromise a sensor node and can obtain all its information.
2. Jammers can move that jammed locations can be changed by the mobile jammers.
3. The jammers are uncoordinated and unsynchronized.so it may happen that successfully jamming attackers have to move while unsuccessful ones remain still.
4. jammers continuously emit RF signals to fill the wireless channel,so that traffic may be blocked. A jammer can do this by either preventing sensor nodes to send sensor readings, or by preventing the reception of traffic at the BSs.
5. A Jammer does not have information about the whole network and it cannot jam the entire network.
6. Jammers can flood the BS with packets,so that it cannot receive packets from sensor nodes.
7. The attacker cannot be captured.

V.DYMO MULTIPATH ROUTING PROTOCOL

Our multipath routing protocol is an extension of DYMO (Dynamic MANET on-demand routing protocol which is based on DYMO is basically an enchancement of the AODV protocol .In the multipath route discovery process if several route. The DYMO agent of its route table,which enables extending the path selection algorithm to make traffic dispersion.multiple paths between source- destination pair will be link disjoint route. So that nodes can be common for two or more paths. Multipath extension of DYMO routing protocol proposed introduces the advertised hop count to prevent loops and a header extension to identify the path.Last hop is the destination neighbour.The path is identified with the pair next-hop / last-hop. During the request phase,every intermediate node has to save the path to the to the request the packet's originator in order to send the corresponding reply message to it.Every intermediate node registers all the paths with different last hope though they may arrive through the same neighbour. During the reply phase, when the destination node receive a rout request it sends the reply back through the neighbour node from which it received the packet;the last-hop value is the same one contained in the request packet.The first path used by each intermediate node with this last hop is the valid path and determines its next hop; the node removes the other paths with the same next hop although with a different last hop. After the rout discovery process, every node will have the one or more routes for every possible destination.

VI.SIMULATION ANALYSIS

In order to simulate the proposed techniques, because it provides a comprehensive environment for designing protocols, creating and animating experiments and analyzing the results of these experiments.

Simulation Setup: After getting request messages, these sensor nodes send their sensing reports to the BSs. This traffic between sensor nodes and BSs is called legitimate traffic. The jammers try to jam the wireless channel, so they continuously emit noisy radio signals for interfering with legitimate traffic signals. The value of PHY-NOISE-FACTOR for jammers is set to 50.Jammers also try to flood the BSs. So they cannot receive yhe legitimate data from sensor nodes such traffic from jammers to BSs is called jamming traffic.

Analysis Metrics: Legitimate traffic throughput is the amount of sensing information sent in a particular time period by the sensor nodes to the BSs.This is measured in terms of Bits/Sec. Jamming traffic throughput is the amount of data sent in particular time period by the - jammers to the BSs for jamming it.This is measured in terms of Bits/Sec.

Result: Legitimate traffic throughput decreases on increasing number of attackers.our hybrid model gives better legitimate traffic throughput than using single defense technique of BS replication or a combination of BS replication with evasion defense techniques in WSN.The ybrid model gives less jamming traffic throughput as compered to using single defense technique of BS replication or a combination of Bs replication with evasion defense techniques in WSN.

VII. CONCLUSION

A hybrid model of defense against BS jamming attack in WSNs.This hybrid model combines 3 defense techniques which are BS replication ,BS evasion from jammed location to unjammed location and multipath routing between sensor node and BSs.The simulation results indicate that legitimate traffic throughput between sensor nodes and BSs.increases, and jamming traffic throughput created by the jammers for jamming BSs decreases after the implementation of the hybrid model.Any single defense technique in WSN. Though there are overheads of increasing network setup cost, communication cost,and transportation cost, these overheads are acceptable and reasonable in comparison to the effects of mobile jamming attacks. Our hybrid model,the use of controlled BS evasion based on reactive approach can give better results, and we are currently doing an implementation of this approach in the hybrid model.

REFERENCES

[1]. J.Deng,R.Han and S.Mishra." Enhancing base station security in wireless sensor networks",Technical Report CUCS 951 – 03, Department of Computer science,University of Colorado,CO, 2002.
[2]. C.Perkins,E.Belding-royer and S.Das," Ad hoc on demand distance vector (aodv) routing,"http://www.ietf.org/rfc/rfc3561.txt,July 2003.
[3]. W.Xu,T.Wood,W.Trappe and Y.hang "Channel surfing and spatial retreats:defenses against wireless denial of service".in Procedings of the 2004 ACM workshop on wireless security 2004,pp.80-89.
[4]. I.Chakeres and C.Perkins "Dynamic manet on-demand (dymo) routing",http://www.ietf.org/internet-drafts / draft – ietfmanet-dymo-17.txt,March 2009.
[5]. A.Mainwaring,J.polastre,R.Szewezyk,D.Culler, and J.Anderson,"Wireless sensor networks for habitat monitoring",In WSNA'02,2002.
[6]. James Carlson,Richard Han,Shandong Lao,Chaitanya Narayan,nad Sagar Sanghani,"Rapid prototyping of mobile input devices using wireless sensor nodes",In WMCSA'03,Monterey,California,USA,October 2003.
[7]. A.Wood and J.Stankovie,"Denial of service in sensor networks",IEEE computer Oct.2002.
[8]. QualNet 4.0 user's Guide Scalable Network Technologise.,Inc .,DEC 2006.