BRAM: A New Bidirectional Routing Abstraction Model for identifying Intruders over Multiple Sensing Networks

BANASMITA MOHARANA [#1], Mr. S K SHARMA [*2], Mr. S K PADHI [*3]

Department of Computer Science & Engineering,
Konark Institute of Science & Technology,
Khurda, Bhubhaneshawar (Orissa).

Abstract

The migration to wireless sensor networks from wired network has been a global trend in the past few decades. For identifying the suspicious objects or intruders in wireless sensor networks there was no proper system until an Intrusion Detection System (IDS) has been proposed. With the implementation of these new IDS, the malicious, incorrect or anomalous moving objects are easily identified in WSN.Wireless sensor networks are generally categorized into two types of networks like Homogeneous based network and other one is Heterogeneous based networks. In this current paper we consider the intrusion detection problem on heterogeneous WSN model. We have applied the bidirectional routing concept in order for the better routing over the existing two protocols AODV and OSPF technologies. For implementing the current problem, we used Qualnet 5.0 Simulator on two different sensing models like SSDM (Single Sensing Detection Model) and MSDM (Multiple Sensing Detection Model). We also proposed and implemented a new intrusion-detection system named Enhanced Adaptive ACKnowledgment Scheme (EAACKS) specially designed for MANETs in this paper. Our simulation results using Qualnet Simulator 5.0 clearly tells the comparison between single sensor homogeneous and multiple sensor heterogeneous networks.

Keywords

WSN, IDS, Multiple Sensing System, Homogeneous Networks, Heterogeneous Networks.

1. Introduction

A Wireless Sensor Network (WSN) is a collection of several nodes ranges from a few to several hundreds and even thousands of nodes, where each and every group of nodes is connected either to single sensor or group of sensors. Sensor network typically has several parts which is clearly shown in figure 1.

1. A radio transceiver device with an inbuilt internal antenna or device connected to an external antenna.
2. A microcontroller
3. An electronic circuit board for interfacing mainly with the sensors and an energy source, usually a battery or an embedded form of energy harvesting.

Sensor may be vary in size when compared with different type of sensors just like of a shoebox down to the size of a grain of dust. The amount for purchasing of single sensor nodes is similarly variable in its price, ranging from a few to hundreds of dollars, depending on the complexity of the individual sensor nodes. While deploying any sensor some valuable resources like energy, memory, computational speed and communication bandwidth mainly depends on size and cost of the sensor what we use. The topology (I.e. arrangement of nodes) of the WSNs can vary from a basic star network to an advanced mesh network. The propagation technique

between the nodes of the wireless network can be routing or flooding [1], [2].

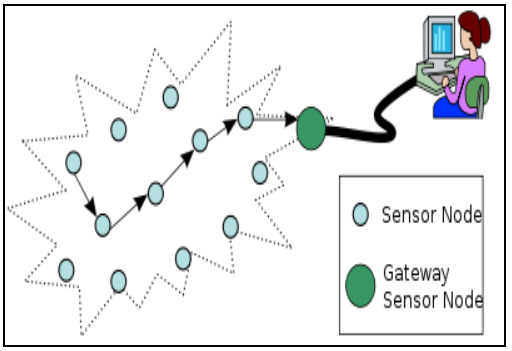


Fig.1. Represents the typical multi-hop wireless sensor network architecture

Recently with the huge usage of wireless sensor networks in a variety of applications, a lot of research efforts have been made to develop sensor hardware and network architectures in order to effectively deploy WSNs.For the general purpose network deployment, normal WSN cannot able to fulfill the needs like sensing range, transmission range, and bandwidth range for sensing the data remotely. To achieve this, it is very crucial to identify the impact parameters of network on its performance w.r.t application specifications. In CSE and telecommunications, wireless sensor networks are an active research area with numerous workshops and conferences arranged each year for the improvement of its performance[3],[4].

Intrusion detection (i.e. Object Tracking)

Object Tracking in a Wireless Sensor Networks can be regarded as a network monitoring system for identifying the attacker who is invading secretly in network domain.

In a WSN, there are two ways to detect an object (i.e., an attacker or intruder):

1. single-sensing detection and
2. multiple-sensing detection

a) In the single-sensing detection, system with the help of single sensor, the intruder can be successfully detected by a single sensor.

b) In the multiple-sensing detection, the intruder can be detected only in the presence of multiple sensors

For some applications, the sensed information which is provided by a single sensor might not be adequate for identifying the attacker. This occurs because individual sensors can only sense small portion of the attacker. For example, in order to identify the location of an intruder, it requires at least three sensors' sensing.

2. Related Work

In this section, we will find the information which was very near to our current intruder detection system in detail.

Intrusion detection

An **Intrusion detection system** (**IDS**) is internet software which is mainly deployed on the hardware designed to detect any unwanted attempts to access, manipulating, and/or disabling of computer mainly through a network. An intrusion detection system is mainly used to identify several types of malicious behaviors that can easily compromise the security and trust of a computer system. Some of the attacks include network attacks against vulnerable services, host based attacks such as privilege escalation attack, unauthorized logins attack and attempting to access some invalid files like viruses and worms.

IDS are mainly composed of several components:

1. Sensors: This is used for generating security events.

2. Console: Which is used to monitor events and alerts, while controlling the sensors.

3. Central Engine

Which is mainly used for recording the events logged by the sensors in a database and use a system of rules to generate alerts from security events received.

Intrusion detection system software is basically executed and deployed in wireless sensor networks. The development of such a variety of wireless sensor networks was originally motivated by military applications such as battlefield surveillance and attacker identification through sensor which is clearly shown in figure 2. However, now a days these wireless sensor networks is also used in many civilian application areas, including environment and habitat monitoring, healthcare applications, home automation, and traffic control.

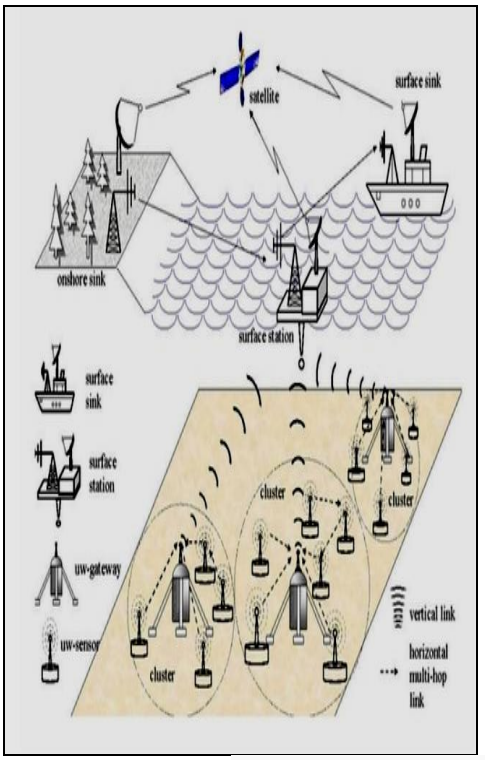


Fig.2. Represents the Military application which uses wireless sensor network

3. Proposed Multiple Sensing Detection Model

In this section, we present our work, the Multiple Sensing Detection problem which is used for identifying attackers which are present in the Multi Hop Wireless Sensor Networks.

In the multiple sensing we deploy a number of sensor nodes .And each sensor will form a cluster of sensor and then they will handle by their local host node. After getting all the local node information it will go to the main server. Then main server will take that input as parameter and execute the one appropriate event which will effect to all.

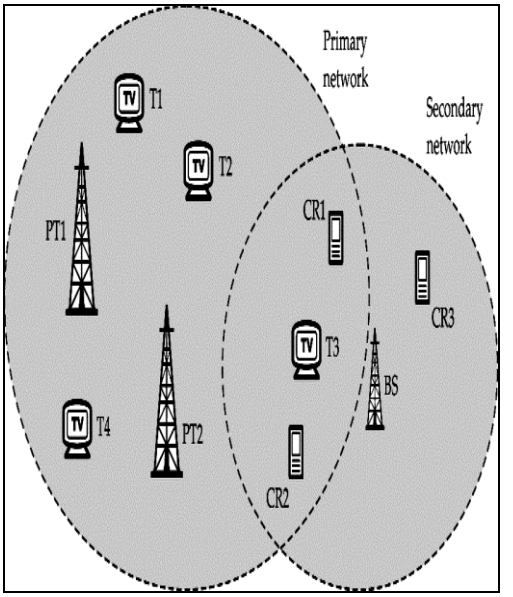


Fig.3. Represents the architecture of Multiple Sensing Detection

Bidirectional Routing Abstraction Model (BRAM)

We present a very new framework known as bidirectional routing abstraction model (BRAM),

which provides improved connectivity and routing performance in asymmetric networks. BRAM model seems to improve the efficiency of off-the-shelf routing protocols typically designed for bidirectional networks to function efficiently on asymmetric networks. To this end, BRAM provides a bidirectional abstraction of the underlying uni-directional links.

The main central feature of BRAM is a new adaptive and scalable technique to maintain reverse routes for unidirectional links. The rest of this section describes this central technique and explains how BRAM provides the necessary functionality to enable routing protocols to operate on asymmetric networks.

While it is always non- trivial to find reverse routes for unidirectional links in an asymmetric network. For instance, the **Distributed Bellman–Ford Algorithm** is a well-known distance-vector algorithm to obtain the shortest routes between pairs of nodes in a bidirectional network. This algorithm always has many practical advantages because it doesn't work synchronously and it is guaranteed to converge eventually if the network is not partitioned and remains stable for a sufficient time. In this proposed algorithm, For example a node B broadcasts its currently known distances to other nodes in the network to its neighbors. When a node A receives this distance-vector message from one of its neighbors say B, it recalculates its minimum distances to other nodes as follows:

If the current known shortest distance from A to another node C is more than one hop longer (to include the hop) than the distance advertised by B to C, then A discovers a new shortest path to C through B. However, the above algorithm fails in the presence of unidirectional links. For instance, if but not , then A would never receive the distance-vector message from B and thus will never be able to discover the shortest hop path to C through B. BRAM finds reverse routes through a modified version of the above algorithm called the Reverse Distributed Bellman–Ford Algorithm (RDBFA). As the name implies, RDBFA operates by reversing the direction of route discovery; that is, each node aims to find the shortest distance from other nodes to itself rather than from itself to other nodes. In the previous example, node B tries to learn the shortest path through which other nodes can reach it. B achieves this when it hears A's reverse-distance vector broadcast saying that C can reach A in hops; B discovers that C can reach B through A in hops since .If, at B, the previous known route from C is longer than hops, B can now record the new hop route from C. Furthermore, if there is a unidirectional link, then C can learn

This figure illustrates show distance vectors are propagated in RDBFA, enabling nodes to discover reverse routes. In this example, node B discovers the reverse route B! C! A of unidirectional link A! B. about this new reverse route to B from B's next reverse-distance- vector broadcast. Each entry in the distance vector includes two values: the length of the shortest route from a node and the address of the first hop in the shortest route from that node. Including the first-hop information provides two benefits:

A) It enables a node to compute the reverse route to its in-neighbors based on local state even though the node cannot always compute the reverse route for other nodes' in-neighbors due to the reversed direction of routing state.

B) As in [5] and [6], it enables RDBFA to avoid routing loops and prevent the counting-to-infinity problem that affects classical distance vector algorithms

EAACKS Algorithm

EAACKS algorithm which is proposed in this paper mainly consists of three parts, namely,

1) ACK,
2) Secure ACK (S-ACK), and
3) Misbehavior Report Authentication (MRA).

In order to distinguish different packet types in different schemes, we included a 2-b packet header in EAACK. According to the Internet draft of DSR [7], [8], there is 6 b reserved in the DSR header. In EAACK, we use 2 b of the 6 b to flag different types of packets. This scheme is clearly shown in the figure.4, which clearly represents system flow of EAACK Scheme.

1. ACK

As we discussed before in figure 4, ACK scheme is basically an end-to-end acknowledgment scheme. It acts as a part of the hybrid scheme in EAACK, aiming to reduce network overhead when no network misbehavior is detected. In Fig. 5, in ACK mode, node S first sends out an ACK data packet *Pad*1 to the destination node D [9].

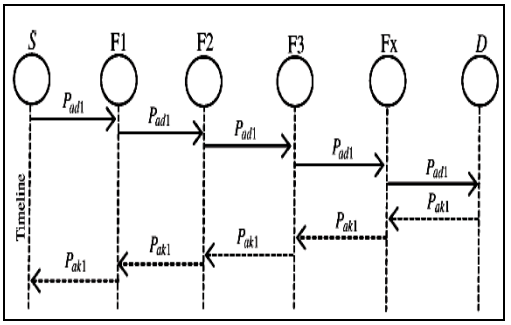


Fig.4. Represents the system flow of EAACK scheme

If all the intermediate nodes along the route between nodes S and D are cooperative and node D successfully receives *Pad*1, node D is required to send back an ACK acknowledgment packet *Pak*1 along the same route but in a reverse order [10].

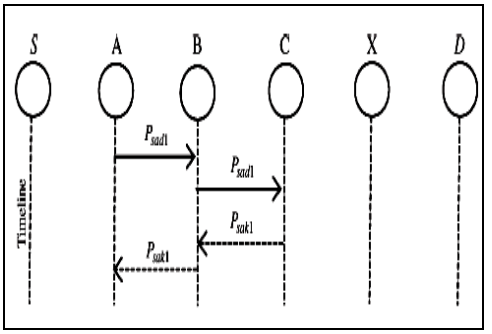


Fig.5. ACK scheme: The destination node is required to send back an acknowledgment packet to the source node when it receives a new packet.

2. S-ACK

The S-ACK scheme is an improved version of the TWOACK scheme proposed by Liu *et al.* [11]. The principle is to let every three consecutive nodes work in a group to detect misbehaving nodes. For each and every three consecutive nodes in the route, the third node is required to send an S-ACK acknowledgment packet to the first node. The intention of introducing S-ACK mode is to detect misbehaving nodes in the presence of receiver collision or limited transmission power.

3. MRA

The MRA scheme is mainly designed to resolve the weakness of Watchdog when it fails to detect misbehaving nodes with the presence of false misbehavior report. The false misbehavior report can be generated by malicious attackers to falsely report innocent nodes as malicious. This attack can be lethal to the entire network when the attackers break down sufficient nodes and thus cause a network division. The core of MRA scheme is to authenticate whether the destination node has received the reported missing packet through a different route [12].

4. Implementation Modules

Implementation is the stage where theoretical design is converted into practical by dividing the whole task into several modules. The following are the several modules that are used in this application. They are as follows

a. Constructing Sensor Network
b. Packet Creation
c. Find authorized and un authorized port
d. Constructing Inter-Domain Packet Filters
e. Receiving the valid packet

a) Constructing Sensor Network Module:

In this module, we are going to connect the network .Each node is connected the neighboring node and it is independently deployed in network area. And also deploy the each port no is authorized in a node.

b) Packet Creation:

In this module, browse and select the source file. And selected data is converted into fixed size of packets. And the packet is send from source to detector.

c) Packet Creation:

In this module the intrusion detection is defined as a mechanism for a WSN to detect the existence of inappropriate, incorrect, or anomalous moving attackers. In this module check whether the path is authorized or unauthorized. If path is authorized the packet is send to valid destination. Otherwise the packet will be deleted. According port no only we are going to find the path is authorized or Unauthorized.

d) Constructing Inter Domain Packet Filters :

In this module if the packet is received from other than the port no it will be filtered and discarded. This filter only removes the unauthorized packets and authorized packets send to destination.

e) Receiving the valid packet:

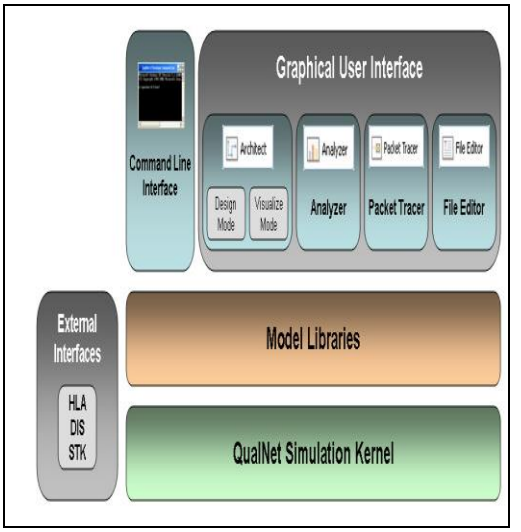
In this module, after filtering the invalid packets all the valid Packets will reach the destination.

5. Experimental Results

We have implemented the proposed concept on Qualnet 5.0 simulator in order to show the performance of our proposed Multiple Sensing Detection model is very accurate in identification of attacker when compared with various existing models.

5.1 QualNet 5.0 Architecture

Figure.4 clearly illustrates the QualNet architecture. A high-level description of the various components is provided below.



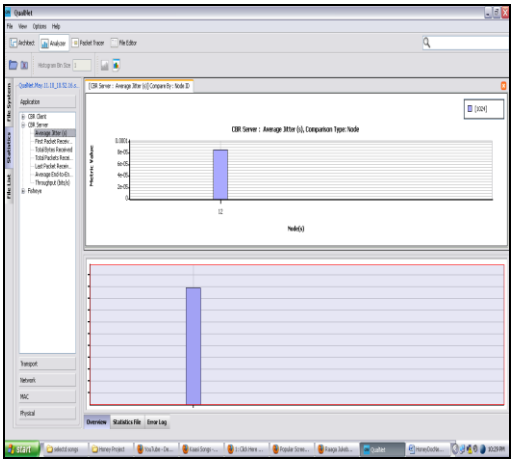
5.2 Simulation Environment

The simulation evaluates the performance of Reactive Routing Protocols using Bidirectional Routing Abstraction Search Technique. The simulations have been performed using QualNet version 5.0, software that provides scalable simulations of Wireless Networks.

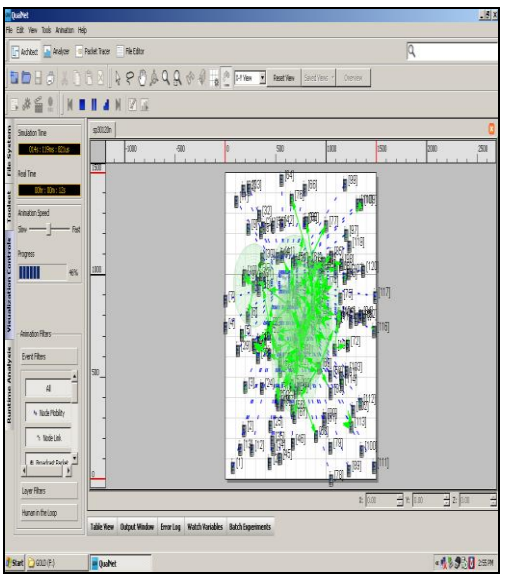
In our simulation, we consider a network of 150 nodes that are placed in an area of 1000m X1000m. The duration of each run is 1500 simulated seconds. The mobility model uses the random waypoint model. The radio model used is the *two ray* model. We change the mobility rate by setting different values to pause time as 0, 30, 60, 90 simulated seconds. Here, a pause time of zero means continuous mobility and 900 seconds reflects stable nodes. The maximum moving speed can be 10m/s. We run simulations covering each combination of pause time and moving speed. Traffic sources are

constant- bit-rate, sending 6 UDP packets a second. Each packet is 512 bytes long, thus resulting 2K byte per second data transfer rate for each session.

Main User Interface of QualNet 5.0 Simulator



Simulation Report of Mobility: Grid Parameter: speed



6. Conclusion and Future Scope

In this paper ,we have conclude that Bidirectional Routing Abstraction can play an important role in controlling flooding in route searching to improve performance of network based on local network information. This project thesis results show that the proposed approach of bidirectional routing abstraction for multiple sensing detection model achieves better performance than single sensing detection model and a lot more existing intrusion detection models. This work can be extended for other protocols with different metrics for different parameters and mobility conditions. Our simulation does indeed succeed at the challenges it set out to address. Our sensor network simulation provides APIs which enable rapid sensor network development, and the graphical tooling enables real-time visual debugging. It is our belief that the architecture of this product is sufficiently in the realm of extensibility and adaptability that it forms a valuable framework for development of sensor network simulations for all types of environmental anomalies, network protocols, and node types.

As a future work, to increase the merits of our research work, we plan to investigate the following issues in our future research:

1) There is a Possibility of adopting hybrid cryptography techniques to further reduce the network overhead caused by digital signature.

2) Examine the possibilities of adopting a key exchange mechanism to eliminate the requirement of predistributed keys.

3) Testing the performance of EAACKS in real network environment instead of software simulation.

7. References

[1] Dargie, W. and Poellabauer, C., "Fundamentals of wireless sensor networks: theory and practice", John Wiley and Sons, 2010 ISBN 978-0-470-99765-9, pp. 168–183, 191–192.

[2] Sohraby, K., Minoli, D., Znati, T. "Wireless sensor networks: technology, protocols, and applications, John Wiley and Sons", 2007 ISBN 978-0-471-74300-2, pp. 203–209.

[3]http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6550437.

[4]http://www.thinkmind.org/index.php?view=article&articleid=icn_2014_3_40_30195

[5]C. Cheng, R. Riley, S. Kumar, and J. Garcia-Lunes-Aceves, "A loopfree extended Bellman-Ford routing protocol without bouncing effect," in Proc. ACM SIGCOMM, Aug. 1989.

[6]T. Clausen and P. Jacquet, "Optimal link-state routing," RFC 3626, Oct. 2003.
[7] D. Johnson and D. Maltz, "Dynamic Source Routing in *ad hoc* wireless networks," in *Mobile Computing*. Norwell, MA: Kluwer, 1996, ch. 5, pp. 153–181.

[8] N. Kang, E. Shakshuki, and T. Sheltami, "Detecting misbehaving nodes in MANETs," in *Proc. 12th Int. Conf. iiWAS*, Paris, France, Nov. 8–10, 2010, pp. 216–222.

[9] Nat. Inst. Std. Technol., Digital Signature Standard (DSS) Federal Information Processing Standards Publication, Gaithersburg, MD, 2009, Digital Signature Standard (DSS).

[10] TIK WSN Research Group, The Sensor Network Museum—Tmote Sky. [Online]. Available: http://www.snm.ethz.ch/Projects/TmoteSky

[11] K. Liu, J. Deng, P. K. Varshney, and K. Balakrishnan, "An acknowledgment-based approach for the detection of routing misbehavior in MANETs," *IEEE Trans. Mobile Comput.*, vol. 6, no. 5, pp. 536–550, May 2007.

[12] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," in *Proc. 6th Annu. Int. Conf. Mobile Comput. Netw.*, Boston, MA, 2000, pp. 255–265.

8. About the Authors

Banasmita Moharana is currently pursuing her 2 Years M.Tech (CSE) in Computer Science and Engineering at Konark Institute of Science & Technology, Khurda, and Bhubhaneshawar (Orissa). Her area of interests includes Networks security and Information Security.

Mr. S K Sharma is currently working as Sr. Assistant Professor, Dept. Of MCA at Vignan Institute of Information Technology, Duvvada, Visakhapatnam. His research interests include Networks, Information Security, Data Mining and Cloud Computing.

Mr. S K Padhi is currently working as Associate Professor, Dept. Of Computer Science and Engineering at Konark Institute of Science & Technology, Khurda, and Bhubhaneshawar (Orissa). His research interests include Networks, Information Security, Data Mining and Cloud Computing.