ISSN:2348-2079

Volume-5 Issue-1

International Journal of Intellectual Advancements and Research in Engineering Computations

SRDD AD-Secured Routing Data Delivery by anonymous detection in wireless sensor networks

Ms.N.Pavethra, Ms.S.Ezhilarasi, Ms.V.Gunasundari, Ms.V.Kalaiyarasi, Ms.R.Sangeetha

[*]Assistant Professor, Department of Electronics and Communication Engineering, Maharaja Engineering College, Avinashi.
Email:pavethra.n@gmail.com

[**]Students,
Department of Electronics and Communication Engineering, Maharaja Engineering College, Avinashi.
Email: honeyvibgyorkalai@gmail.com

ABSTRACT

In this paper, we investigate the Secured Routing and data delivery between the source–destination pairs in wireless sensor networks (WSN), where Anonymous node expose their selfish behaviors, i.e., forwarding or dropping data services.

Manage the Anonymous node information in terms of its available resources, the employed incentive mechanism and the quality-of-service (QoS) requirements, and the other terms of their historical behaviors. In this framework, we used DSR Routing for Route Detection and Route Maintenance. Under the Anonymous Detection management, in this framework we used Random Key Pre-distribution (RKP) a security key management for secure path selection criterion is designed to select the most reliable and shortest path in terms of Routing available resources.

KEYWORDS: dropping data, quality of service, route detection and maintenance, secure path.

1. INTRODUCTION

1.1WIRELESS SENSOR NETWORKS

Sensor networks are highly distributed networks of small, lightweight wireless nodes, deployed in large numbers to monitor the environment or system by the measurement of physical parameters such as temperature, pressure, or relative humidity.

Building sensor has been possible by the recent advances in Micro-Electro-Mechanical Systems (MEMS) 1 technology. Each node of the sensor networks consists of three sub systems. The sensor subsystems which senses the environment, the processing subsystem which performs local computation on sensed data and the communication subsystem which is responsible for message exchange with neighboring sensor nodes. While individual sensors have limited sensing region, processing power, and energy, networking a large number of sensors rise to robust, reliable, and accurate sensor network covering a wider region.

The network is fault-tolerant because many nodes are sensing the same events. Further, the nodes cooperate and collaborate on their data which leads to accurate sensing of events in the environment. The two most important operation in a sensor network are data dissemination, that is, the propagation

of data/queries throughout the network, data gathering, that is, the collection of observed data from the individual sensor nodes to a sink.

1.2 ROUTING

Routing is the process of selecting path for traffic in a network, or between or across multiple networks. Routing is a performed for many types of networks including circuit switched networks, such as the Public Switched Telephone Network (PSTN), Computer networks, such as the internet as well as in networks used in public and private transportation, such as the system of streets, roads and highways in national infra structure.

In packet switching networks, routing is the high-level decision making that directs network packet from their source towards their destination through intermediate network nodes by specific packet forwarding mechanisms. Packet forwarding is the transit of logically addressed packets from one network interface to another. Intermediate nodes are typically network hardware devices such as routers, bridges, gateways, firewalls, or switches. General-purpose computers also forward packets performs routing, although they have no specially optimized hardware for the task the routing process usually directs forwarding on the basis of routing tables, which maintain a record of the routes to various networks destination

1.3 NETWORK SECURITY

A specialized field in the computer networking that involves securing a computer networks infra structure. Network security is typically handled by a network administrator or system administrator who implements the security policy, network software and hardware needed to protect a network and the resources accessed through the network from unauthorized access and also ensured that employees have adequate access to the network and resources to work.

A network security system typically relies on layers of protection and consists of multiple components including networking monitoring and security software in addition to hardware appliances. All components work together to increase overall security of the computer networks.

2. AMD

AMD address the problem of identifying and isolating misbehaving nodes that refuse to forward packets in multi-hop ad hoc networks.

It develops a comprehensive system called Audit-based Misbehavior Detection (AMD) that effectively and efficiently isolates both continuous and selective packet droppers. The AMD system integrates reputation management, trustworthy route discovery, and identification of misbehaving nodes based on behavioral audits.

Compared to previous methods, AMD evaluates node behavior on a per-packet basis, without employing energy-expensive overhearing techniques or intensive acknowledgment schemes. Moreover, AMD can detect selective dropping attacks even if end-to-end traffic is encrypted and can be applied to multi-channel networks or networks consisting of nodes with directional antennas.

Existing solutions for identifying misbehaving nodes either use some form ofper-packet evaluation of peer behavior or provide cooperation incentives to stimulate participation.

Incentive-based approaches do not address the case of malicious nodes who aim at disrupting the overall network operation. On the other hand, per-packet behavior evaluation techniques are based on either transmission overhearing or issuance of per-packet acknowledgements.

These monitoring operations must be repeated on every hop of a multi-hop route.It leading to high communication overhead and energy expenditure. This framework, they fail to detect dropping attacks of selective nature, since intermediate monitoring nodes may not be aware of the desired selective dropping pattern to be detected.

3. SRDD

This scheme is secure against adaptive chosen-message attacks. This scheme enables the intermediate nodes to authenticate the message so that all corrupted message can be detected and dropped to conserve the sensor power. While achieving compromise resiliency, flexible-time authentication and source identity protection, our scheme does not have the threshold problem**.**

In this proposed framework, we used SRDD-AD named Secured Routing and Data Delivery by Anonymous Detection in Wireless Sensor Networks. We investigate the Secured Routing and data delivery between the source–destination pairs in wireless sensor networks (WSN), where Anonymous node expose their selfish behaviors, i.e., forwarding or dropping data services.

Manage the Anonymous node information in terms of its available resources, the employed incentive mechanism and the quality-of-service (QoS) requirements, and the other terms of their historical behaviors. In this framework, we used DSR Routing for Route Detection and Route Maintenance. Under the Anonymous Detection management, in this framework we used Random Key Pre-distribution (RKP) a security key management for secure path selection criterion is designed to select the most reliable and shortest path in terms of Routing available resources.

System architecture

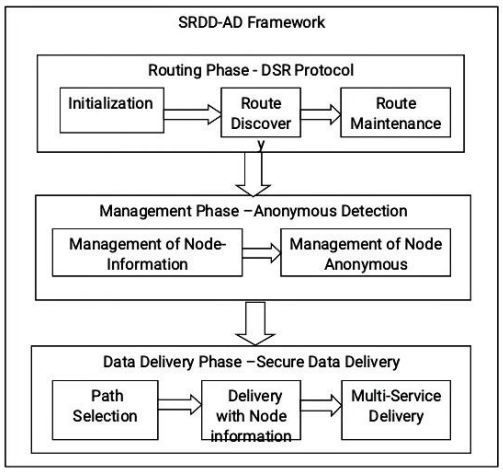

Fig 3.0

3.1.LIST OF MODULES

Network Model
Route Discovery
Data delivery phase
Anonymous Detection

3.2. Network model

In this module used to initialize the nodes in network topology. We used network topology and topography for our network animator window. We have syntax for create nodes in network animator window. Then we can create nodes in two types like random and fixed motions.

In random motion we fixed range for X and Y, fixed particular range then the nodes are randomly generate in that range of window. In fixed motion we give X and Y dimension position for all nodes then all the nodes are fixed in that particular dimension.

Sensor nodes are aware of their own positions. The position information may be based on a global or a local geographic coordinate system defined according to the deployment area.

Determining the position of the nodes might be achieved using a satellite based positioning system such as Global Positioning System (GPS) or one of the energy-efficient localization methods proposed specifically for WSNs.

3.3. Route discovery

Normally the source can find the route when the data is waiting in buffer without route by using the route request and route reply. In this scheme, we are also going to use same method with different style, such as creating the fake route request.

The source will generate fake request with destination address as cooperating neighbor. Source already knows the information, for frequently no reply. But incase if there is reply from any node, then that node will be identified as malicious by using the source routing mechanism. If route is failed means the intermediate node will share the error message. Based on the error message the source node will find another route to destination. With secure route discovery model.

The beacon generator can generate the packet and that packet can be read by any neighbor node, the beacon life is only for one hop. The work of neighbor management unit is

to store the neighbor information into table when it receives the beacon packet from the neighbor.

Here fixed timer for all beacon messages, when neighbor got the beacon messages then send ACK to sender. If the time is got expire the neighbor node info will be deleted from the table.

3.4. Data delivery phase

For delivering multi-services, the sources find some paths by virtue of the traditional routing protocol. Nevertheless, these paths may not be all reliable for successfully forwarding multi services due to the node-selfishness of the relay node within the paths.

Although the relay node represents its behavior of forwarding multi-services, the data information is not the best option to select the most reliable path. When the relay of a few available resources have high energy, their historical behaviors may be the ones of forwarding the multi-services owing to the large incentives, thus leading to their low power. If these relay nodes are selected within the path of delivering multi-services in terms of the node information, the sources should provide large incentives for stimulating the multi-service forwarding of these data and maintaining the reliability of the selected path.

3.5. Anonymous detection

This proposed which integrates the Proactive and reactive defense architectures, and randomly establishing a cooperation with adjacent node. The address of the adjacent node is used as the bait destination address, baiting malicious nodes to send RREP reply messages and identifies the malicious nodes by using the reverse tracing program. Finally the detected malicious node is listed in the anonymous list and notifies the remaining nodes in the network to halt any communication with them. Because some of the traffic data are not reliable, it is critical to find an evidence combination technique to properly fuse together multiple pieces of evidence in presence of both trustworthy and untrustworthy data. Thus, it is necessary to combine multiple pieces of evidences so that both data trust and functional trust can be properly evaluated.

In this work, is used to fuse together multiple piece of evidences even if some of them might not be accurate. As a result, my proposed scheme can reduce packets loss that can be cause by malicious nodes and have better throughput.

4. RESULT

Here we compare Packet delivery ratio. In our modification ratio increased comparing to existing and proposed methods

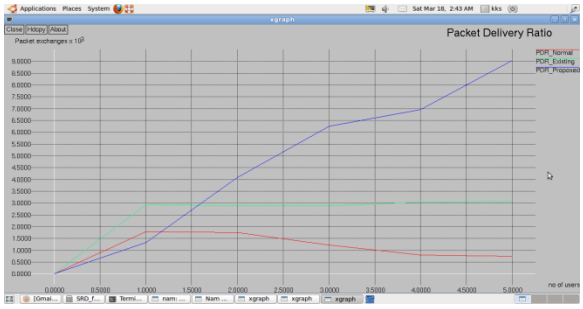

Fig4.0

5.sCONCLUSION

In this paper, we investigate the Secured Routing and data delivery between the source–destination pairs in Wireless Sensor Networks (WSN), where Anonymous node expose their selfish behaviors, i.e., forwarding or dropping data services.

Manage the Anonymous node information in terms of its available requirements, and the other terms of their historical behaviors. In this framework, we used DSR Routing for Route Detection and Route Maintenance. Under the Anonymous Detection management, in this framework we used RandomKey Pre-distribution (RKP) a security key management for secure path selectioncriterion is designed to select the most reliable and shortest path in terms of Routing available resources.

REFERENCES

T. Shu and M. Krunz, “Detection of malicious packet dropping in wireless Ad Hoc networks based on privacy-preserving public auditing, “ in Proc. 5th ACM Conf. Security Privacy Wireless Mobile Netw., 2012, pp. 87–98.

V.-N. Padmanabhan and D.-R. Simon, "Secure trace route to detect faulty or malicious routing," SIGCOMM Comput. Commun. Rev.,vol. 33, no. 1, pp. 77–82, 2003.

S. Marti, T. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile Ad Hoc networks," in Proc. 6th Annu. Int. Conf.Mobile Comput. Netw., 2000, pp. 255–265.