
Shobha.K, Mamtha Jadhav.V
P.G Student. Assistant Professor

Abstract—This paper research on to Develop and simulate a secure efficient dynamic routing using protocol for the wireless sensor network. Efficiency is an important factor because the sensor networks devices are energy constrained and may not charged again after drained, so the routing protocol should not consume more energy and drain the sensor nodes energy. We propose to use the OSPF routing protocol for the wireless sensor network. We propose the way to use OSPF for the wireless sensor network. Each network node updates the link information to their neighbors and based on this link information, the route is learnt. Simulate the Established network using any of the available simulators. User will configure the number of nodes, position of nodes in the network and the communicate range of the nodes etc using this viewer. User also views the routing table at any node, the message success ratio, the energy consumed at nodes at the viewer. Node need to know the routing path to another node. The routes are maintained in the routing table. To learn the route, Node uses the OSPF routing agent, which sends link messages to nearby neighbors. Form the link state messages the routing path are learnt dynamically. Link message handler module listens on the network for any link message and provides to OSPF Routing Agent. OSPF Routing Agent implements the OSPF Routing. In OSPF Routing each node requires complete topology information Link state information must be flooded to all nodes.

Index Terms—Open Shortest Path First (OSPF), Link-State Packets, Backbone Area of OSPF, Area Border Routers (ABRs), OSPF Routing Agent.

I. INTRODUCTION

Wireless Sensor networks have features [1] like low cost, flexibility, fault tolerance, high sensing fidelity, creating many new and exciting application areas for remote sensing. So [2], wireless sensor network has emerged as a promising tool for monitoring the physical world with wireless sensor that can sense, process and communicate. There are many issues of wireless sensor network which need to be addressed [2]. As researchers are working in the area of wireless sensor network, more and more data is collected, the refined the models and techniques will become in the future. On the Internet [3] and other infrastructure networks, there is a clear separation of roles: there are end systems (nodes) and intermediate systems (routers, switches and the like). But in sensor networks each node is potentially a router for some other nodes. This creates an entirely new set of vulnerabilities in the network layer. For example, routers can become neglectful, in that they selectively do not forward packets from other nodes, or they can become selfish, in the sense that they prefer to give preference to their own packets. Such behaviors are often the result of denial-of-service attacks. A WSN consists of an array of sensors [4], interconnected by a wireless communication network. Sensor data is shared between these sensor nodes and used as input whose function is to extract the relevant information from the available data. Main objectives of sensor networks include reliability, accuracy, flexibility, cost effectiveness and ease of deployment. Each node [3] has one or more sensing unit. All nodes in the sensor network act as information sources, sensing and collecting data samples from their environment. The main components [5] of sensors consist of a sensing unit, a processing unit, a transceiver, and a power unit. As with the popularity of wireless networks, importance of sensor networks has grown. Wireless sensor networks have a lot in common with wireless ad hoc networks, but many of the security mechanisms designed for ad hoc networks simply won’t fly on networks of sensors. Unlike in ad hoc networks, not every pair of nodes in a sensor network needs to communicate. Also, in ad hoc networks many security mechanisms usually rely on public key algorithms, which are sometimes too expensive in terms of resources for sensor networks. We could attempt to adapt a secure routing protocol based on secret-key cryptography, but it would impose non-trivial packet overheads in addition to necessitating the gathering of node state information. Routing is the one which shows path to the packets. Routing[6] misdirection is an attack whereby malicious nodes advertise false routes to either inject artificial traffic into the channel, direct traffic to a fraudulent base station or node, eliminate part of the network by overtaxing its resources or avoid forwarding packets entirely. Such an attack can be foiled using authentication, network monitoring and redundancy techniques. Authentication mechanisms based on distributed certification authorities have been proposed, but these have been shown to be tough to implement in real-world environments. Some network monitor applications can have neighbor nodes listen to both the sender and forwarder of a message, and notify the sender if the exact packet is not forwarded to the next hop of the route within a specific time limit. Unfortunately, packet comparison is not enough, since aggregation points may delay transmissions until enough information has been collected. Even if the time threshold is long enough, aggregated data will probably not match
transmitted data. This will result in mischaracterizing the aggregation node as a “bad actor.”

A. Battery Attacks

Attacks [3] targeting the battery exhaustion of nodes are termed attacks on “system lifetime” [9]. Why would an attacker bother? Suppose, for example, a sensor network is deployed as an early-warning system for biological or chemical attacks. Because of the widely distributed nature of the sensor network, it would be almost impossible for a terrorist to physically destroy it. An easier option would perhaps be to insert a few misbehaving nodes that force the legitimate sensors to work continuously until their batteries are totally exhausted. Then the terrorist [9] could proceed with his real-world attack, undetected. There is a difficult trade-off in the case of sensor networks. These devices [3] have a triple role: as data collectors, processors and forwarders. The goal of the network is to be working as long as possible, in order to transfer information from the objects to the sinks. But the objects “want” to participate in the network as little as possible, in order to stay active for a longer lifetime. This creates conflict for the node, and sets the stage for battery attacks. Selfish behavior and “unfairness” in cooperative protocols can be considered weak forms of denial-of-service attacks, and there are many others more advanced such as sleep deprivation attacks. Link layer protocols for channel arbitration can even be manipulated to exhaust batteries or simply degrade network performance. For example, channel jamming results in transmission errors, which make nodes, retransmit data and increase transmission power to overcome noise. Another form of attack is interrogation. A selfish node may continuously request channel reservation. In cooperative MAC protocols, like those based on IEEE 802.11, neighbor nodes are forced to reply to those requests and thus eventually consume all their energy reserves. Most, if not all of the problems in current approaches to securing networks of smart objects arise from the fact that security has been designed as an add-on, not as an integral part of the network architecture. The resource constraints common to wireless sensor networks often deprive the security architect of one of our favorite tools: public key cryptography. Fortunately, even the “lowest” [10] modern sensors are getting better processors and more memory, enabling them to “speak IP” and participate in the global public key infrastructure. Good work, too, has been done on optimizing and miniaturizing public key algorithms. elliptic curve approaches can sometimes work well. When memory is just too tight, or processors just too weak, however, clever work-around and hard compromises are needed.

II. RELATED WORK

A. Existing System

There is no security for wireless networks Wireless Sensor Networks (WSNs) are rapidly emerging as an important new area in wireless and mobile computing research. OSPF used for the wired network, for router to learn the routes dynamically. Applications of WSNs are numerous and growing, and range from indoor deployment scenarios in the home and office to outdoor deployment scenarios in adversary’s territory in a tactical battleground. For military environment, dispersal of WSNs into an adversary’s territory enables the detection and tracking of enemy soldiers and vehicles. For home/office environments [11], indoor sensor networks offer the ability to monitor the health of the elderly and to detect intruders via a wireless home security system. In each of these scenarios, lives and livelihoods may depend on the timeliness and correctness of the sensor data obtained from dispersed sensor nodes. As a result, such WSNs [11] must be secured to prevent an intruder from obstructing the delivery of correct sensor data and from forging sensor data. To address the latter problem, end-to-end data integrity checksums and post-processing of sensor data can be used to identify forged sensor data. The focus of this is on routing security in WSNs. Most of the currently existing routing protocols for WSNs make an optimization on the limited capabilities of the nodes and the application-specific nature of the network, but do not any the security aspects of the protocols. Although these protocols [6] have not been designed with security as a goal, it is extremely important to analyze their security properties. When the defender has the liabilities of insecure wireless communication, limited node capabilities, and possible insider threats, and the adversaries can use powerful laptops with high energy and long range communication to attack the network, designing a secure routing protocol for List of various application [7] areas of WSN are as follows.

1. Military Situation Awareness
2. Battlefield Surveillance
3. Communication, Command,
4. Control, Targeting Systems
5. Fish Monitoring

B. Routing Protocols

Routing protocols were created for routers. These protocols have been designed to allow the exchange of routing tables, or known networks, between routers. There are a lot of different routing protocols, each one designed for specific network sizes, so I am not going to be able to mention and analyze them all, but I will focus on the most popular. The two main types of routing: Static routing and Dynamic routing Routed Protocols. We all understand that TCP/IP, IPX-SPX are protocols used in a Local Area Network (LAN) so computers can communicate between with each other and with other computers on the Internet. Chances are that in your LAN you are most probably running TCP/IP. This protocol is what we call a “routed” protocol. The term "routed" refers to a protocol that contains specific type of information that allows it to be passed on from one network to another. In the example of TCP/IP, this protocol contains the destination IP Address to which the packet is destined to go, therefore you can construct a data packet and send it across to another computer on the Internet. Wireless Sensor network were first implemented in Military areas. Now a day’s large range of
applications of sensor network has become integral part of our life. Lists a few application areas as described by the researchers in their studies. Static routing allows routing tables in specific routers to be set up by the network administrator. Dynamic routing uses Routing Protocols that dynamically discover network destinations and how to get to them. Dynamic routing allows routing tables in routers to change if a router on the route goes down. Examples of Routing Protocols are RIP, EIGRP and OSPF. There are three basic types of routing protocols. Distance-vector Routing Protocols: Distance-vector Routing Protocols use simple algorithms that calculate a cumulative distance value between routers based on hop count. Example: RIP. Link-state Routing Protocols: Link-state Routing Protocols use sophisticated algorithms that maintain a complex database of internetwork topology. Example: OSPF Hybrid Routing Protocols: Hybrid Routing Protocols use a combination of distance-vector and link-state methods that tries to incorporate the advantages of both and minimize their disadvantages. Example: EIGRP. Types of routing protocols are mainly RIP & OSPF.

III. PROPOSED SYSTEM

Open Shortest Path First (OSPF) [8] is a link-state routing protocol that was developed for IP networks and is based on the Shortest Path First (SPF) algorithm. OSPF is an Interior Gateway Protocol (IGP). We propose to Develop & simulate a secure efficient dynamic routing using protocol for the wireless sensor network. Efficiency is an important factor because the sensor networks devices are energy constrained and may not charged again after drained, so the routing protocol should not consume more energy and drain the sensor nodes energy. We propose to use the OSPF routing protocol for the wireless sensor network. OSPF routing is previously used for the wired network, for router to learn the routes dynamically. We propose the way to use OSPF for the wireless sensor network. Each network node updates the link information to their neighbors and based on this link information, the route is learnt. Simulate the Established secure efficient routing protocol for the wireless sensor network using simulator.

In an OSPF network, routers or systems within the same area maintain an identical link-state database that describes the topology of the area. Each router or system in the area generates its link-state database from the link-state advertisements (LSAs) that it receives from all the other routers or systems in the same area and the LSAs that itself generates. An LSA is a packet of information generated by a neighbor and path costs. Based on the link-state database, each router or system calculates a shortest-path spanning tree, with itself as the root, using the SPF algorithm. So we can propose this OSPF for efficient dynamic routing in wireless sensor network. In the control plane, a routing protocol, e.g., BGP, OSPF, exchanges routing state updates and enables routers to compute the best paths towards various destinations. During this phase, an attacker can modify or inject malicious control messages leading to incorrect computation of routing paths. In the data plane, the routers forward the data along the paths computed in the control plane. Even if an attacker is not successful during the control phase, he can choose not to use the correct routing paths and forward data along routes that benefit him. Research shows that, attacks on the control plane can be mitigated by ensuring message integrity and, attacks on the data plane can be mitigated by ensuring route integrity. Earlier works have addressed these two problems independently with many interesting solutions. However, due to the nature of these solutions, network architects cannot deploy security at both planes without increasing the overhead on the network. Since the application of WSN in many areas, so security for routing required. This paper mainly concentrates on that. For Routing purpose we can use many standard protocols available. Especially for dynamic routing OSPF can be used in order to provide secure dynamic routing in WSN. Dynamic routing uses a dynamic routing protocol to automatically select the best route to put into the routing table. So instead of manually entering static routes in the routing table, dynamic routing automatically receives routing updates, and dynamically decides which routes are best to go into the routing table. It’s this intelligent and hands-off approach that makes dynamic routing so useful. Dynamic routing protocols vary in many ways and this is reflected in the various administrative distances assigned to routes learned from dynamic routing. These variations take into account differences in reliability, speed of convergence, and other similar factors.

A. OSPF has the following key advantages over RIP

Compared with distance-vector routing protocols such as the Routing Information Protocol (RIP), OSPF is more suitable for serving large, heterogeneous internetworks. OSPF can recalculate the routes in a short amount of time when the network topology changes. With OSPF, you can divide an Autonomous System (AS) into areas and keep area topologies separate to decrease the OSPF routing traffic and the size of the link-state database of each area. OSPF provides equal-cost multipath routing. You can add duplicate routes to the TCP stack using different next hops.

B. Link-State Packets

Link State Packet is a packet of information generated by a network router in a link state routing protocol that lists the router’s neighbors. There are different types of Link State Packets; those are what you normally see in an OSPF database. Router Link, Summary Link, Network Link, External Link. Uses Area Border Routers (ABRs). An ABR is a router that connects one or more OSPF areas. It is considered a member of all areas it is connected to. An ABR keeps multiple copies of the link-state database in memory, one for each area to which that router is connected. Below is a configuration for an ABR. Network statements describe which interfaces we should include in OSPF LSA (Link-state advertisement), and to which areas they correspond.
OSPF uses link state packets (LSPs) which are special datagram’s that determine the names of and the cost or distance to any neighboring routers and associated networks.

Fig.1 ABR Network Diagram [12]

Fig.2 Link-State Packets Diagram [12]

Fig.3 Backbone Area Diagram of OSPF [12]

User will configure the number of nodes, position of nodes in the network and the communicate range of the nodes etc using this viewer. User also views the routing table at any node, the message success ratio, the energy consumed at nodes at the viewer. Routing table dynamically updates and it cannot be modified by anyone. Node need to know the routing path to another node. The routes are maintained in the routing table. To learn the route, Node uses the OSPF routing agent, which sends link messages to nearby neighbors. Form the link state messages the routing path are learnt dynamically. Link message handler module listens on the network for any link message and provides to OSPF Routing Agent. Prepare performance charts using the main parameters such as, the number of messages exchanged, message delivery ratio, the nodes energy.

OSPF Routing Agent
OSPF Routing Agent implements the OSPF Routing. In OSPF Routing Each node requires complete topology information Link state information must be flooded to all nodes

The working of OSPF in terms of steps is given below.
1. Each node establishes a relationship (“adjacency”) with its neighbors
2. Each node generates link state advertisements (LSAs) which are distributed to all nodes
3. Each node maintains a database of all received LSAs (topological database or link state database), which describes the network has a graph with weighted edges
4. Each node uses its link state database to run a shortest path algorithm (Dijkstra’s algorithm) to produce the shortest path to each network. Finally simulate the established network using any of the simulators available.

IV. ADVANTAGES

Dynamic routing uses a dynamic routing protocol to automatically select the best route to put into the routing table. So instead of manually entering static routes in the routing table, dynamic routing automatically receives routing updates, and dynamically decides which routes are best to go into the routing table. It's this intelligent and hands-off approach that makes dynamic routing so useful. Dynamic
routing protocols vary in many ways and this is reflected in the various administrative distances assigned to routes learned from dynamic routing. These variations take into account differences in reliability, speed of convergence, and other similar factors.

V. DESIGN DOCUMENT

A. Sequence Diagram

Fig. 5a. User Configuring Nodes
When node is initialized, the node broadcasts link status message.

Fig. 5b. User Requesting For A Route to Destination Node from a Source Node

Fig. 5c. Calculating the Route

VI. CONCLUSION

From this we can conclude that we can first develop and then simulate a secure efficient dynamic routing using protocol in wireless sensor networks. We can use this proposed techniques which is cost effective, secure and simpler to configure. In order to provide security to the unwanted threats in the networks we can use OSPF dynamic routing protocol technique in Wireless sensor networks. Simulate the secure dynamic routing in wireless sensor networks in any available simulators. We can guarantee that it will be definitely useful and cost effective.

VII. FUTURE ENHANCEMENT

Implementation of the proposed system to develop a secure efficient dynamic routing using OSPF protocol in wireless sensor network. Finally simulate the proposed system using any of the available simulators to get the results of the system. The simulation results will be analyzed and compared.

REFERENCES


[5] Vol. 32, No. 6 ACTA AUTOMATICA SINICA November, 2006 Energy-aware System Design for Wireless Sensor Network1) ZHAO Lei1,2 ZHANG Wei-Hong3 XU Chao-Nong1,2 XU Yong-Jun1,2 LI Xiao-Wei1,2.


[12] IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 11, NO. 2, FEBRUARY 2012 Hop-by-Hop Routing in Wireless Mesh Networks with Bandwidth Guarantees Ronghui Hou, Member, IEEE, King-Shan Lui, Senior Member, IEEE, Fred Baker, and Jiandong Li, Senior Member, IEEE

[13] Detection and Localization of Multiple Spoofing Attackers in Wireless Networks Jie Yang, Student Member, IEEE, Yingying Chen, Senior Member, IEEE, Wade Trappe, Member, IEEE, and Jerry Cheng.

AUTHOR BIOGRAPHY

Mrs. Shobha K. P.G Student Department of Computer Science at MSRIT Bangalore, INDIA. Presently doing IIIRd Sem M.Tech in Computer Science and Engineering at MSRIT, Bangalore, INDIA. 

Mrs. Mamatha Jadhav V Assistant Professor Department of Computer Science at MSRIT Bangalore, INDIA.