

Protected Routing in Wireless Sensor Networks: A study on Aimed at Circulation

M.Rajesh
Assistant Professor, Department of Computer Science & Engineering, KRS College Of Engineering,Vandavasi.

1. Abstract
The aim of this paper is to discuss secure routing in Wireless Sensor networks. I have made an endeavor to present an analysis on the security of Directed Diffusion, a protocol used for routing in wireless sensor networks. Along with this the paper also discusses the various attacks possible on this routing protocol and the possible counter-measures to prevent theses attacks.

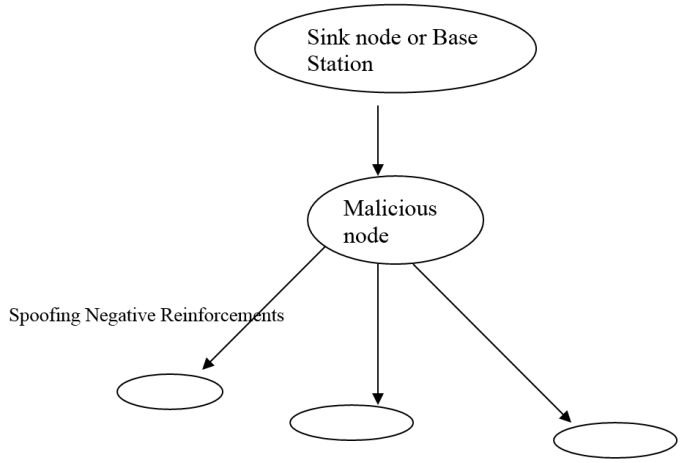
2. Introduction
The technological advancements in wireless communication and microelectronics have resulted in a growing interest in the field of wireless sensor networks. A sensor network involves deploying an array of sensors for distributed monitoring of real time events. The sensor networks have limited energy, as the sensor nodes are battery powered. The sensor nodes also have limited memory and computational capability and can be deployed in remote areas or inhospitable terrain. There has been an increasing use of sensor networks for life critical applications such as monitoring patients in hospitals and military applications. These applications make it important to have a good security infrastructure for sensor networks. The deployment of these networks in military applications and the limited power and memory, make the design of a security protocol very challenging. In this paper security issues in Directed diffusion are addressed. Directed Diffusion is a novel routing protocol for sensor networks. A look-in to possible attacks and counter measures is provided. Section 3,briefly covers the directed diffusion protocol followed by a discussion on the possible attacks on this routing protocol. The paper is concluded with a brief analysis on the possible countermeasures to prevent such attacks.

3. Directed Diffusion: An insight
Directed Diffusion [1] is a data-centric, interest-based routing protocol. An interest is a request for a specific type of data. For ex: In a sensor network to monitor various properties of water in a lake, the interest could be a request for data on toxins to be sent every 10 seconds for the next 50 seconds from a particular area of the sensor network. This interest message would be sent as a packet. The node that sends out interests is referred to as the sink node. The sink node resends these interest packets periodically. A base station node normally does the interest dissemination. This node broadcasts its interests to all its neighbors in the network. This process is referred to as interest-dissemination. The interests consists of the following parameters:
Type of data required by the sink node
Area of sensor network from which the data is required (X, Y co-ordinates)
How often the data needs to be sent to the sink node? This is referred to as data refreshing rate.
Expiration time
Based on these parameters for the interest dissemination, a gradient is set-up in the reverse direction for data flow. This gradient is set-up in response to the interest dissemination instantiated by the sink node. This process of interest dissemination and the corresponding gradient establishment continues until we reach the nodes generating the events. These are referred to as source nodes. The data is routed through paths, which have a higher gradient value. Those nodes, which send out data more frequently to the sink node, would be positively reinforced. This would mean that the paths to these nodes would obtain higher gradient values, by increasing the data refresh rate. The sink node must refresh and reinforce the interest once it begins to receive data from the source node. Also each node stores a copy of the interest it receives in an interest cache, before it forwards the interest. This is done to avoid routing loops and repeated flooding. Thus the directed diffusion is based on data centric routing where the sink node broadcasts the interest.

4. Attacks on directed diffusion
The possible attacks on directed diffusion protocol can be classified under:
Denial of Service attacks
Modification and spoofing of routing information
Dropping or selective forwarding of data
In the following sections these attacks along with the possible countermeasures against these attacks is discussed.
Denial Of Service attacks
The simplest form of the denial of service attack would require an attacker to deploy a malicious node with a

powerful transmitter and a large battery power. This would enable the attacker to jam the communications in the entire sensor network with his powerful transmitter. A normal malicious node would only be able to jam the communication link in its immediate vicinity.

A second form of denial of service attack would involve spoofing negative reinforcements. A malicious node could spoof negative reinforcements to certain nodes. If the latter nodes communicate with the base station or a sink node via the malicious node, they would be denied service to the base station because of the spoofed negative reinforcements that they received from the malicious node. The figure below depicts this:



Blocked sensor nodes

Fig1: Simple DOS attack

Modification and spoofing of routing information

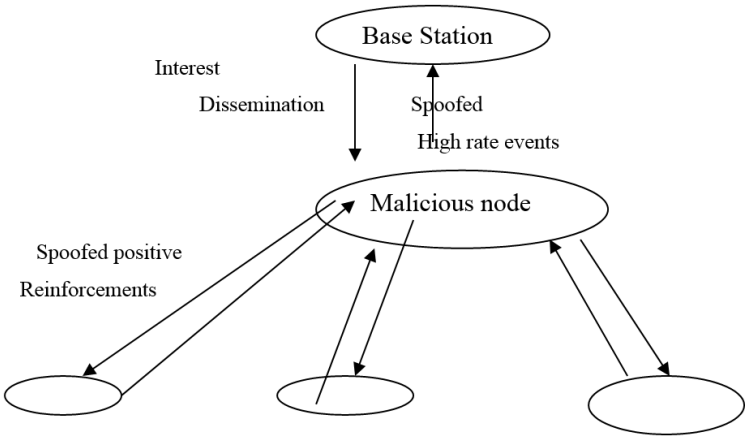
In Directed Diffusion the routing is done on the basis of interest dissemination and the corresponding gradient establishment. If a malicious node receives interests from the base station, it could replay the interest with itself listed as the base station. This would enable the malicious node to receive a copy of the events, which are sent to the base station.

A malicious node can influence the other nodes to route data through it by spoofing positive and negative reinforcements and false data events. For example consider that a malicious node receives interests from the base station or a sink node. It adopts the following procedure

Rebroadcasts the interests to its upstream nodes. Upstream is the direction from sink node to source node.

Sends strong positive reinforcements to the upstream nodes. This would enable the malicious node to receive a steady flow of events from the its upstream nodes Send spoofed events at a high data rate to the sink node or base station This would make the base station to positively reinforce the malicious node as against the alternate routes, as the node is generating a steady stream of events. Thus the malicious node has successfully been able to include itself in the path of the base station and observes all packets sent to the base station

The figure below depicts this:



Nodes generating and sending event data as they have a high gradient path to malicious node

Fig2: Spoofing Positive Reinforcements

(Also enables easy selective forwarding)

Dropping or selective forwarding of data

Most sensor networks are multi hop networks. These networks rely on all the nodes to correctly forward the messages. In this scenario a malicious node could drop or selectively forward only certain messages. If a malicious node drops all messages, it would be as good as the node not being present in the network. The sensor network is designed to adapt to this. But a more severe form of this attack would be if a malicious node selectively forwards only certain messages. With the spoofed positive and negative reinforcements discussed in the previous section, we saw how a malicious node can successfully include itself in the path of data flow. This now makes selective forwarding trivial. The malicious node can now forward only certain messages and suppress the rest. Thus once a malicious node includes itself in the path of data flow, the selective forwarding can be easily achieved.

Countermeasures

The following are some of the problems with the directed diffusion protocol, which make the protocol more vulnerable:

The interest packet in the Directed diffusion protocol does not have any information regarding the sink node that generated the interest. There could be some provision to specify the identity of the sink node in the interest packet. This along with the encryption of the data would make spoofing interests difficult.

The data packets received from the source nodes contain no information regarding the identity of the source node. This information coupled with encryption of data would to some extent prevent malicious nodes from spoofing high data rates to the base station.

One of the useful steps that can be taken to prevent some of the attacks is to use encryption at the link layer. The nodes could share a key with the base station and thus data flow could be authenticated. It is vital that efficient symmetric key cryptographic schemes be employed. Public key cryptography would be too expensive and infeasible to use in sensor networks with the limited memory and computational capabilities of the nodes. The link layer encryption would prevent most external attacks against sensor networks. Internal attacks from compromised nodes are harder to defend against. One novel scheme of preventing some of the attacks would be for the base station to limit the number of neighbors a node can have. This would restrict the compromised node to communicating with its immediate neighbors. It would be very hard to defend against a denial of service attack if the malicious node has a strong transmitter. It is vital to design the security infrastructure into the routing protocol rather than trying to retrofit. With the challenges of limited node power and memory, the security for sensor networks is an open research issue.

CONCLUSION

This paper addresses some of the security issues for routing in sensor networks by taking an example of the directed diffusion protocol for analysis of the attacks and general possible countermeasures. Link layer encryption may be sufficient for external attacks, but compromised nodes within the network would be the most difficult attacks to prevent. This has to be achieved with careful and conscious designing of the routing protocol.

REFERENCES

[1] C. Intanagonwiwat, R. Govindan, and D. Estrin, “Directed Diffusion: A Scalable and Robust Communication paradigm for Sensor Networks,” Proc. ACM MobiCom, Boston, MA, pp. 42-49, 2000.

[2]. Chris Karlof and David Wagner, “Secure Routing in Wireless Sensor Networks,” Adhoc Networks, Volume1, Issues 2-3, pp: 293-315, September 2003.

The IISTE is a pioneer in the Open-Access hosting service and academic event management. The aim of the firm is Accelerating Global Knowledge Sharing.

More information about the firm can be found on the homepage:
http://www.iiste.org

CALL FOR JOURNAL PAPERS

There are more than 30 peer-reviewed academic journals hosted under the hosting platform.

Prospective authors of journals can find the submission instruction on the following page: http://www.iiste.org/journals/ All the journals articles are available online to the readers all over the world without financial, legal, or technical barriers other than those inseparable from gaining access to the internet itself. Paper version of the journals is also available upon request of readers and authors.

MORE RESOURCES

Book publication information: http://www.iiste.org/book/

Academic conference: http://www.iiste.org/conference/upcoming-conferences-call-for-paper/

IISTE Knowledge Sharing Partners

EBSCO, Index Copernicus, Ulrich's Periodicals Directory, JournalTOCS, PKP Open Archives Harvester, Bielefeld Academic Search Engine, Elektronische Zeitschriftenbibliothek EZB, Open J-Gate, OCLC WorldCat, Universe Digtial Library , NewJour, Google Scholar