Secure Data Transmission Routing Protocol for Multicasting

Bharath V N
8th Sem, Information Science & Engineering Department
Coorg Institute of Technology
Ponnampet, South Kodagu
vnbharath307@gmail.com

Navile Nageshwara Naveen
Lecturer, Computer Science & Engineering Department
Coorg Institute of Technology
Ponnampet, South Kodagu
nnnaveen.nag@gmail.com

Abstract

As sensor network edge closer towards wide-pread deployment, security issues become a central concern. So far, more research has focused on making sensor networks for feasible and useful, but not concentrated on security. Recently technological advancement in the field of nanotechnology have increased the computation power of the wireless nodes while adhering to the energy constraints. This made use of Wireless Sensor Networks (WSNs), more widespread, used in applications such as area monitoring, industrial monitoring, vehicle detection or military monitoring. SPIN, Sensor Protocol for Information via Negotiation, is one of the widely used efficient routing protocol in WSNs that completely ignores the security aspect. SPIN overcome the performance deficiencies of conventional protocols by implementing data negotiation, nodes communicating with each other about the data that they have send already and also the data they still need to obtain, and resource adaption, that is, nodes monitor and adapting to changes in their own energy resources. This project mainly propose an alternate routing protocol which routes the data similar to SPIN, but with additional security features. The energy performance characteristics, large number of nodes and percentage of malicious nodes are compared with SPIN and MS-SPIN in NS2.

I. Introduction

Wireless networks of sensors are likely to be widely deployed in the future because they greatly extend our ability to monitor and control the physical environment from remote locations. Such networks can greatly improve the accuracy of information obtained via collaboration among sensor nodes and on- line information processing at those nodes.

Wireless sensor networks improve sensing accuracy by providing distributed processing of vast quantities of sensing information (e.g., seismic data ,acoustic data, high-resolution images, etc.). Wireless sensor networks can also improve remote access to sensor data by providing sink nodes that connect them to other networks, such as the Internet, using wide-area wire- less links. If the sensors share their observations and process these observations so that meaningful and useful information is available at the sink nodes, users can retrieve information from the sink nodes to monitor and control the environment from afar. We, therefore, envision a future in which collections of sensor nodes form ad hoc distributed processing networks that produce easily accessible and high-quality information about the physical environment. Each sensor node operates autonomously with no central point of control in the network, and each node bases its decisions on its mission, the information it currently has, and its knowledge of its computing, communication and energy resources. Compared to today's isolated sensors, tomorrow's networked sensors have the potential to perform with more accuracy, robustness and sophistication. Several obstacles need to be overcome before this vision can become a reality. These obstacles arise from the limited energy, computational power, and communication resources available to the sensors in the network.

• ***Energy***: Because wireless sensors have a limited supply of energy, energy-conserving communication protocols and computation are essential.
• ***Computation***: Sensors have limited computing power and therefore may not be able to run sophisticated network protocols.
• ***Communication***: The bandwidth of the wireless links connecting sensor nodes is often limited, on the order of a few hundred Kbps, further constraining inter-sensor communication.

Sensor Protocols for Information Via Negotiation (SPIN) [3] and [7] proposed a family of adaptive protocols called Sensor Protocols for Information via Negotiation (SPIN) that disseminate all the information at each node to every node in the network assuming that all nodes in the network are potential base-stations. This enables a user to query any node and get the required information

immediately. The SPIN family of protocols uses data negotiation and resource-adaptive algorithms. Nodes running SPIN assign a high-level name to completely describe their collected data (called meta-data) and perform meta-data negotiations before any data is transmitted. This assures that there is no redundant data sent throughout the network. The semantics of the meta-data format is application and is not specified in SPIN. The SPIN family is designed to address the deficiencies of classic coding by negotiation and resource adaptation. The SPIN family of protocols is designed based on two basic ideas:

1. Sensor nodes operate more efficiently and conserve energy by sending data that describe the sensor data instead of sending all the data; for example, image and sensor nodes must monitor the changes in their energy resources.

2. Conventional protocols like coding or gossiping based routing protocols waste energy and bandwidth when sending extra and un-necessary copies of data by sensors covering overlapping areas.

SPIN's meta-data negotiation solves the classic problems of coding, and thus achieving a lot of 8 energy efficiency. SPIN is a 3-stage protocol as sensor nodes use three types of messages ADV, REQ and DATA to communicate. ADV is used to advertise new data, REQ to request data, and DATA is the actual message itself. SPIN has four types they are:

1. SPIN – PP (Point to point communication)
2. SPIN - EC (Three hop transmission)
3. SPIN - BC (Transmission of data in timing sequence)
4. SPIN - RL (Multiple request.)

II. Requirements for Sensor Network

Security
In this section, we formalize the security properties required by sensor networks, and show how they are directly applicable in a typical sensor network.

Data Confidentiality
A sensor network should not leak sensor readings to neighbouring networks. In many applications (e.g. key distribution) nodes communicate highly sensitive data. The standard approach for keeping sensitive data secret is to encrypt the data with a secret key that only intended receivers possess, hence achieving confidentiality. Given the observed communication patterns, we set up secure channels between nodes and base stations and later bootstrap other secure channels as necessary.

Data Authentication
Message authentication is important for many applications in sensor networks. Within the building sensor network, authentication is necessary for many administrative tasks (e.g. network reprogramming or controlling sensor node duty cycle). At the same time, an adversary can easily inject messages, so the receiver needs to make sure that the data used in any decision making process originates from the correct source. Informally, data authentication allows a receiver to verify that the data really was sent by the claimed sender.

Data Integrity
In communication, data integrity ensures the receiver that the received data is not altered in transit by an adversary. In SPINS, we achieve data integrity through data authentication, which is a stronger property.

Data Freshness
Given that all sensor networks stream some forms of time varying measurements, it is not enough to guarantee confidentiality and authentication; we also must ensure each message is fresh. Informally, data freshness implies that the data is recent, and it ensures that no adversary replayed old messages. We identify two types of freshness: weak freshness, which provides partial message ordering, but carries no delay information, and strong freshness, which provides a total order on a request-response pair, and allows for delay estimation.

III. Modified Routing Protocol (ms-spin)

Even though SPIN protocols provide a very attractive approach of routing which is very energy efficient, they do not address any security challenges which deemed them unsuitable for using in places which involve sensing of sensitive information such as in military application. In this paper, we provide an alternate routing algorithm which routes data in a way similar to SPIN, but with additional security features. We use the concept of encrypting the group address of the node which multi casts the data. This encrypted group address is sent along with the ADV packet. We also use a private key while encrypting the group address so that only the authentic nodes can decrypt it. After decrypting it, the node which needs the data listens at the group address and gets the data. This process continues till the time data is not

disseminated in the network.

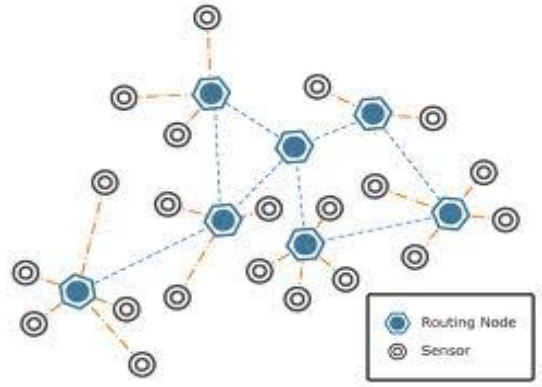

FIG 1: MS-SPIN NETWORK

3.1 Terminology Used

Node: For routing the information from the Source to the Sink.

Cluster Head: It consists of the following properties:

a) It IS nearest to the secondary Centralized Authority (CA).
b) It is chosen by the secondary CA and is responsible for proper allocation of all the IP addresses to the nodes.

Secondary CA: It is a Secondary Centralized Authority

a) A fixed node and Responsible for choosing the Cluster Head and checking the authenticity of the Cluster Head.
b) Keeps information about all the nodes in its cluster and forwards this information to the Cluster Head when required.

Main CA: It is the main Centralized Authority

a) A fixed node and Responsible for coordinating with all the secondary CA in allocating the IP address to the rest of the nodes.
b) Responsible for checking the authenticity of all the secondary CAs.

Find-packet: This is a packet broadcasted by a node so as to find out the nearest secondary CA.

Ack-packet: It is a packet sent by the Sink node to the Source node informing it that the initial packet has been received.

End-packet: This is a packet sent by the source node to the destination node signifying the end of data transfer.

Assumptions

1. The proposed protocol MS-SPIN was implemented with the following.
2. One main CA is present in the network.
3. Multiple secondary CAs are present in the network.
4. Secondary CA has information about all the nodes in its cluster.

5. Each node has a private key that will be used to check its authenticity.

6.It is assumed that the number of IP addresses available in our address space is 232. This is because we are assuming 32 bit IP addresses. Hence based on our protocol, which allocates 2 IP addresses (explained later); the total number of sensor nodes is limited to 231.

7. Every node must have 2 IP addresses to take part in the communication process. One is allocated when it becomes part of the network and the second by its secondary CA.

3.3 Initial Phase

Nodes will send a Find-packet to all the Secondary CAs in its range

a. The Secondary CA will respond back to the node which broad casted the packet with an Ack-packet

b. The node will decide the Secondary CA nearest to it and will then send back another Ack-packet informing the Secondary CA about its choice.

3.4 Setup Phase

Once the initial phase is over and the node is now in the sensor network, it initiates a setup phase which includes the allocation of secondary IP addresses to the nodes which will be later used in the Data Communication phase as a multicast address.

Algorithm 1: CA_Main_SetupO

a. Detect all the Secondary CAs by sending a Find-packet.
b. The Secondary CA will respond back to C.A.MAIN which broadcasted the packet with an Ack-packet which includes the number of IP address needed by it.
c. Check if all the Secondary CAs are authentic by checking their private keys. If not then report back (to the office) so thathuman intervention.
d. Send IP addresses to the Secondary CA according to the request sent by it, and also make sure that the number of requests does not exceed the total available IP addresses with Main CA.

Algorithm2: Ca_SecondarLSetupO

a. Once the Main CA contacts, it then sends the request about the number of IP addresses needed by it.

b. Detect the best node in its cluster. Maintain a list of nodes based on this criterion Check if the best node selected is authentic (checking the private key), if not then report to the Main CA.
c. The best node becomes the Cluster Head.
d. Send the IP addresses to be allocated to the nodes in the cluster and also their existing IP addresses to the Cluster Head.
e. After the process is completed send an Ack packet to the Main CA.

Algorithm 3: Cluster_ Head _SetupO

a. Get information about all the nodes In its cluster from the Secondary CA.
b. Communicate with all the nodes whose information was given to it, check if the node is authentic or not, if not report to the Secondary CA. Otherwise send the node its secondary IP address.
c. After successful allocation send an Ack packet to the Secondary CA.

3.5 Data Communication Phase

a. Once the initial phase and the setup phase are completed, each node will then run this algorithm to carry out its communication.
b. Each node in the system will either be sensing data, involved in the routing process, or waiting for some data.
c. If a node has some data it will fIrst be sending that data before accepting new data.

Algorithm 4: Data_ReceiveO

a. When a node receives an adv packet and if the node is waiting for some data it will check if it needs that particular data (needs it for itself or for sending to other node). If not, it will ignore the packet.
b. If it is waiting for data and the adv packet is of the data it needs or it has to route the data, then the node will decrypt the IP address (secondary IP address sent encrypted by the node) and send a request at the secondary IP address.
c. The node will wait till the transfer is over. This end of transfer is signalled by a packet called end-packet.

The node will now check if the data it just received was meant for it or not, if yes it will again get back to the work it was previously doing before it got interrupted and if no it will then send this data to its neighbours.

Algorithm 5: Data_SendO

a. The node will send an adv packet about the data it wishes to send and also include its secondary IP address in encrypted form.
b. It will then wait for any request from its neighbours. Both the source and the nodes which want the data will be listening at the secondary IP address of the source.
c. The source node will multicast the data at its secondary IP address.
d. After the data transfer is over the source node will get back to the work it was doing before getting interrupted.

IV. Conclusion

A secure data routing protocol, MS-SPIN, for static wireless sensor networks. MS-SPIN comprises of mainly three phases: the initial phase, the setup phase and the data transfer phase. The frrst phase consists of basically identifying all the nodes and assigning a secondary CA to each node. This phase involves the division of all the nodes into clusters. The second phase involves choosing a cluster head for each cluster and then checking the authenticity of the identified nodes. In this phase, the nodes are assigned their secondary IP addresses that are used during the data transfer phase. The third phase involves the actual data transfer between the nodes using multicast. So we can say comparing to SPIN ,MS SPIN is more secure alternative.

References

[1] I. F. Akyildiz, W. Su, Y. ankarasubramaniam, and E. Cayirci, "A survey on sensor networks," IEEE Communications Magazine, Vol. 40, Issue 8, pp. 102- 114, August 2002.
[2] G. Pottie and W. Kaiser, "Wireless Sensor Networks", Communications of the ACM, Vol. 43, Issue 5, pp. 51- 58, May 2000. [3] W. Hu, V.N. Tran, N. Bulusu, C. Chou, S. Jha, A. Taylor, "The design and evaluation of a hybrid sensor network for Cane-Toad monitoring", in Proceedings of the 4th International Symposium on Information Processing in Sensor Networks, Los Angeles, CA, pp. 382- 387, 2005.
[4] S. Hedetniemi, A. Liestman, "A Survey of Gossiping and Broadcasting in Communication Networks, " IEEE Networks, Vol. 18, No. 4, pp. 319- 349, 1988.
[5] W.R. Heinzelman, J. Kulik, and H. Balakrishnan, "Adaptive Protocols for Information Dissemination in Wireless Sensor Networks", in Proc. of 5th annual
ACMlIEEE international conference on Mobile computing and networking, Seattle, Washington, pp. 174-185, 1999.
[6] 1. Kulik, W. R. Heinzelman, and H. Balakrishnan,"Negotiation-based protocols for disseminating information in wireless sensor networks," WirWireless Networks, Vo1.8, pp. 169-185, 2002.[7] http://www.isi.edu/nsnam/ns/[8] IEEE 802.11: Wireless LAN Medium AccessControl (MAC) and Physical Layer (PHY)Specifications.(2007revision).IEEE-SA.

12June2007doi: 10.11 09/IEEESTD.2007.373646.http://standards.ieee.org / getieee802/download/802.11 2007.pdf
.[7] C.Schurgers and M. B. Srivastava. Proceedings of
IEEE MlLCOM," Energy efficient routing in wireless sensor networks", 2008
[8] Shayesteh Tabatabaeil, Mohammad Ali Jabraeil Jamali, Malekan Branch, Malekan, Shabestar, Iranlslamic Azad University "A stable weight-based Routing Algorithm to Increase Throughput in Mobile Ad hoc Networks", 2009.
[9] FANG Wangsheng, ZHANG Tao, CHEN Kang,"A Key Management Scheme for wireless sensor networks Based on Vector Group" School of Information Engineering Jiangxi University of Science and Technology Ganzhou, Jiangxi Province 341000, China, 2009
[10] Deepali Virmani Satbir Jain IJCA Special Issue on MANETs, "Stable Routing for achieving Quality of Service in wireless Sensor Networks" 2010
[11] Zanrree Che-aronl, Wajdi AIKhateeb2 and Farhat Anwar "An Enhancement of AODV Routing Protocol for More Robust Wireless Sensor Network" 2010.