Secure-SPIN: Secure Sensor Protocol for Information via Negotiation for Wireless Sensor Networks

Debao Xiao[1, 2], Meijuan Wei[1], Ying Zhou[2]

[1]Department of Computer Science, HuaZhong Normal University,
Wuhan, Hubei Province, China, 430079
[2]School of Information Engineering, WuHan University of Technology
Wuhan, Hubei Province, China, 430070
Email:dbxiao0227@vip.sina.com, blueice987wmj@yahoo.com.cn, going-zy@163.com

Abstract

Many routing protocols have been proposed for sensor network, but most of them have not designed with security as a goal. Sensor protocol for information via negotiation (SPIN) protocol is a basic data centric routing protocol of sensor networks. In this paper, we present the design of secure-SPIN, a secure extension for the SPIN protocol. We divide secure-SPIN into three phases and use some cryptographic functions that require small memory and processing power to create an efficient, practical protocol. Then we give security analyses of this protocol. It shows that this secure protocol may increase the data communication security in wireless sensor networks.

Keywords-wireless sensor networks; security; SPIN; routing protocol

1 Introduction

Wireless sensor network is becoming an increasingly important technology that will be used in a variety of applications such as public safety, environmental monitoring, public safety, medical, home and office security, transportation, and military[1][2]. Routing protocol in sensor network is very pivotal. SPIN protocol is a basic data-centric routing protocol of wireless sensor networks [3]; though many new algorithms have been proposed for the problem of routing data in sensor networks, most of these protocols have not been designed with security as a goal. Karlof and Wagner[4] propose security goals for routing in sensor networks, give six classes attacks against sensor networks and analyze the security of all the major sensor network routing protocols, at last suggest countermeasures and design considerations. But they do not propose any integrated scheme for a particular routing protocol.

In this paper we focus on secure routing protocol of sensor networks and present the design of secure-SPIN, a secure extension of SPIN routing protocol, which is using some cryptographic functions that require small memory and processing power for data authentication and integration, and we also give security analyses on our secure-SPIN.

2 SPIN Routing Protocol

Sensor Protocol for Information via Negotiation protocol (SPIN) has four types: SPIN-PP, SPIN-EC, SPIN-BC, and SPIN-RL [5]. This paper based on SPIN-PP. In SPIN-PP, Nodes use three types of messages ADV, REQ and DATA to communicate [6]. ADV is used to advertise new data, REQ to request for data and DATA is the actual message itself. The protocol starts when a SPIN node obtains new data that it is willing to share. It does so by broadcasting an ADV message containing meta-data. If a neighbour is interested in the data, it sends an REQ message for the DATA and the DATA is sent to this neighbour node. The neighbour sensor node then repeats this process to its neighbours as a result of which the entire sensor area will get a copy.

Fig.1 [5] shows an example on how this protocol works. It starts by advertising its data to node B (a) from Node A. Node B responds by sending a request to node A (b). After receiving the requested data (c), node B then sends out advertisements to its neighbours (d), who in turn send requests back to B (e, f).

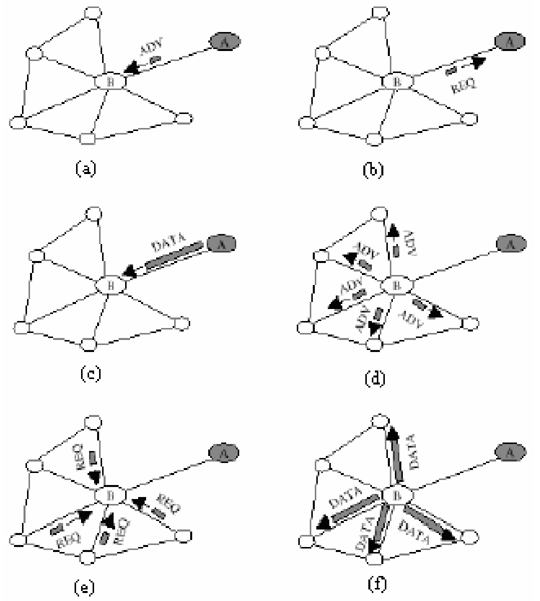

Fig.1. The SPIN-PP Protocol.

0-7803-9514-X/06/$20.00 ©2006 IEEE

The strength of this protocol lies in its simplicity. Each node in the network performs little decision making when it receives new data, and therefore wastes little energy in computation. Furthermore, each node only needs to know about its single-hop network neighbours.

3 Secure-SPIN

3.1 Assumption

We assume that the communication architecture of the sensor network as Fig.2 [1]. The sensor nodes are scattered in a sensor field. Each of these scattered sensor nodes has the capabilities to collect data and route data back to the sink. A sink may be a long-range radio, capable of connecting the sensor network, the sink may also be a mobile node acting as an information sink, or any other entity required to extract information from the sensor network. The sink may communicate with the task manager node, the user, via internet or satellite. We assume that the sink has capabilities similar to the network nodes, except that it has sufficient battery power to surpass the lifetime of all sensor nodes, sufficient memory to store cryptographic keys, and means for communicating with outside networks.

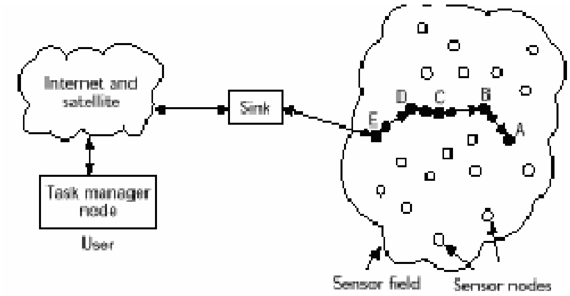

Fig.2. Architecture of the sensor networks.

In addition, in SPIN-PP which has been referred before, when a node broadcasting an ADV message, if all of its neighbours don't have enough power to forward the data, then "data blink spot" will occur. To overcome this, clustering-based SPIN has been proposed. Clustering-based SPIN is a clustering-based protocol that dividing all the sensor nodes to different classes and every class randomly selects sensor nodes as cluster-heads, so the high-energy dissipation in communicating with the sink is spread to all the sensor nodes in the sensor network. So we assume that this secure-SPIN rooting protocol based on the Clustering-based SPIN.

3.2 Notations

With the limited computation resources available in sensor network, we used symmetric key cryptography, which does not involve any cryptographic functions that require large memory and processing power to construct the Secure-SPIN protocols.

The Secure-SPIN protocol is divided into three phases according to SPIN's three messages. We will use the following notation:

(a) AC: Authentication Code;

(b) Ks: sink's privacy key;

(c) Kses: session key;

(d) PSAC: Personal Sensor Authentication Code;

(e) Ki: sensor node's privacy key;

(f) H (): hash function to calculate the hash value;

(g)MAC: Message Authentication Code.

3.3 Detail of Secure-SPIN routing Protocol

The communication patterns within our network fall into four categories: node to cluster-head and cluster-head to sink communication; cluster-head to node and sink to cluster-head communication; sink to all nodes communication.

Each sensor node has a Ki to be used in secure communications, each sink has a Ks. Sink is given the list of all the keys of sensor nodes. And sink also assigns a CDMA code to every sensor node in the sensor field. The task manager node provides the Kses[7] to all of sinks every session, to prevent replay attacks and to keep data freshness. Sink generates the AC by encrypting the Kses with sink's Ks and then hashing the output. Session key is provided by task manager periodically to prevent replay attacks and to keep the data freshness.

$$AC = H\,(E\,Ks\,(Kses)) \qquad (1)$$

Then sink sends AC to all sensor nodes through the cluster-head. And every sensor node generates the PSAC using AC XOR with its privacy key Ki. This process is redone whenever the sink generates a new Kses and broadcasts a new AC.

$$PSA\,C = AC \oplus Ki \qquad (2)$$

We would start by explaining our security protocol between node to cluster-head and cluster-head to sink communication.

First, the node that wants to become a cluster-head needs to be authenticated by the sink using its PSAC. It is the node that who wants to become a cluster-head send a request message to the sink, the request message is a message that contains the request and the node's PSAC, when the sink receives the request message, it gets the node's privacy key according to its PSAC, if the privacy is in the list of sink, the sink can ensure that this node is legal, then it estimates whether the node can be a cluster-head, if it can, the sink will send all nodes' privacy key in this class to the cluster-head.

At ADV message sending phase, in order to avoid an external attacker to advertise, the node which obtains new data that it is willing to share should be encrypt the ADV. For example, if node A would like to share its new data, it first encrypts ADV with its PSAC to get an encrypted ADV, and then send the encrypted ADV to its cluster-head. The cluster-head uses the sensor node A's private key and current AC to decrypt the encrypted ADV to get ADV. Since only the sink and the cluster-head know node A's private key, the cluster-head can trust that the ADV sent by node A is issued by sink. Then the cluster-head checks to see if it possesses all of the advertised data. If not, it sends an REQ message back to node A, asking for all the data it would like to acquire.

Because of the cluster-head has already been authenticated. So at REQ message sending phase, the cluster-head just need to send REQ message back to A.

At DATA message sending phase, if a sensor node wants to send data to it's cluster-head, it first XOR data with its PSAC, then adds MAC [7] at the end of the packet, and then sends the packet to the cluster-head via its own CDMA [7] code. Upon receiving the data, cluster-head first pulls out the respective Ki of that code, using Ki, the sink checks MAC to see if the data is altered. If there is no alteration, then the sink XOR the coming data with Ki and current AC. Result is the original data sent by the sensor node.

This security protocol also can be applied between the sink to cluster-head and cluster-head to node communication. As it is mentioned before, the sink has all sensor node's privacy keys including cluster-head's, so when it wants to communicate with a cluster-head, it just need to see whether it has that cluster-head's privacy key, if it has, it then can communicate with the cluster-head. In the same manner, the cluster-head can communicate with the sensor nodes in its cluster.

In addition, if sink wants to send message to all nodes', it just sends message to the sensor node whose key is in the sink to ensure secure communication.

3.4 Security Analyses

Security properties required by sensor networks include that data confidentiality, data authentication, data integrity, data freshness [8].

In our secure-SPIN routing protocol, we generate AC with a hash function so that the malicious user can never make out it; we encrypt the ADV message with PSAC to realize the data authentication; PSAC is generated by Ki, it makes sure that the data is confidential. With the privacy authentication technology, we set up secure channels between nodes and cluster-head, and cluster-head and sink.

In addition, we use MAC code to ensure data integrity; it makes the receiver believe that the received data is not altered in transit by an adversary.

We also ensure each message is fresh. In our protocol, we use session key to keep data freshness. It ensures that the data is recent, and it ensures that no adversary replayed old messages.

Moreover, we use the CDMA technology to enhance secure communication because of that the CDMA can provide cheap, clear, and energy efficient wireless communication

4 Conclusions

In this paper, we mainly present the design of Secure-SPIN, a Secure Sensor Protocol for Information via Negotiation for wireless sensor network. We divide Secure-SPIN into three phases according to SPIN's three messages. This protocol use PSAC which is generated by Ki, it makes sure the data confidentiality; and the malicious user can never make out the AC as it is generated with a hash function; the protocol is also energy efficient and takes advantage of CDMA codes to enhance security. Moreover it uses XOR operation, which can be accomplished by hardware multiplexer without any additional energy requirement.

In the future, we will do some experiments and validate our conclusions next. We believe that this security routing protocol would increase the data communication security on wireless sensor networks in the nearly future.

References

[1] I. F. Akyildiz, W. Su, Y. ankarasubramaniam, and E. Cayirci, "A survey on sensor etworks," IEEE Communications Magazine, Volume: 40 Issue: 8, pp.102-114, August 2002.

[2] G. Pottie and W. Kaiser, Wireless Sensor Networks. Communications of the ACM, 43(5):51–58, May 2000.

[3] V. D. Park and M. S. Corson, "A highly adaptive distributed routing algorithm for mobile wireless networks," in IEEE INFOCOM '97, 1997, pp. 1405–1413.

[4] C. Karlof, D. Wagner，Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures. Ad Hoc Networks, 2003, 1 (223):2932315.

[5] J. Kulik, W. R. Heinzelman, and H. Balak- rishnan, "Negotiation-based protocols for disseminating information in wireless sensor networks," Wireless Networks, Volume: 8, pp. 169-185, 2002.

[6] M. Esler, J. Hightower, T. Anderson, and G. Borriello, Next century challenges: Data- centric networking for invisible computing: The portolano project at the University of Washington. In Proc. ACM Mobicom, 2000.

[7] H. Çam, S. Ozdemir, D. uthuavinashiappan, and P.Nair, "Energy-efficient security protocol for wireless sensor networks", IEEE VTC Fall 2003 Conference, October 4-9, Orlando, 2003.

[8] J. P. Hubaux, L. Buttyán and S. Capkun, The quest for security in mobile ad hoc networks, in: ACM Symposium on Mobile Ad Hoc Networking and Computing (2001).