5.7 Wireless Sensor Networks – Security Routing Protocol

Routing algorithm is the basis of information transmission and convergence in the wireless sensor networks. As multi-hop networks, wireless sensor networks have especial characteristics, especially in the aspect of security routing and the need for in-depth research. At present, domestic and foreign scholars have proposed a variety of wireless sensor network routing protocols.

5.7.1 Data-Centric Security Routing Protocol and SPIN Protocol

As the wireless sensor networks are data-centric networks, the data-centric routing protocol has been designed for wireless sensor networks. The protocol takes into account the problem of data redundancy and obtains the fused data through collaboration between the nodes, thus improving data transmission efficiency and saves network energy.

Joanna and Wendi et al. proposed SPIN protocol which is a data-centric adaptive routing protocol. In wireless sensor networks, since nodes sensing data have certain similarities, SPIN protocol can effectively reduce the amount of data transmitted and energy consumption in the network through negotiation between nodes. However, SPIN protocol needs to send inspection packet before sending the packet every time, thus causing a large data transmission delay. In addition, SPIN data broadcast mechanism cannot guarantee the reliability of data transmission.

Chalermek and Ramesh designed a directed diffusion routing protocol specifically for wireless sensor networks, which was based on data-centric routing protocol model. The protocol introduces a network “ladder” concept, combining with the local routing protocol for wireless sensor networks communication. Directed diffusion process is divided into query diffusion, data dissemination, and path reinforcement. Since the establishment of directed

diffusion routing requires a flood spread and causes big expense of energy and time, the algorithm is suitable for the scenario, which has a large number of queries but a short time.

Rumor routing that overcomes the problem of excessive spending from establishing forwarding path thought flood spread method was proposed by David and Deborah. Rumor routing basic idea is that time zone sensor node generates agency messages, and agency messages spread outward diffusion along a random path, while the query messages from the sink node also spread along a random path in the network. When the transmission path of agency messages and query messages cross together, there is a full path from a sink node to the event area. Compared with the directed diffusion routing, rumor routing effectively reduces the routing established expense. However, because of rumors that the routing path is generated randomly, the data transmission path is not optimal path, and maybe even routing loops exist.

5.7.2 Location-based Secure Routing Protocol and GPSR, GEAR Protocols

Most location-based routing protocols assumed that each node in the network knows own location information, and location nodes can exchange information with their neighbors, so that nodes can use location information to make routing choice without the need to save the routing table, and the typical protocols are GPSR and GEAR.

GPSR (Greedy Perimeter Stateless Routing) routing algorithm is the method by directly using geographic information to establish the routing path. GPSR algorithm uses a greedy routing strategy, and each node only needs to know the destination node of the packet and the location information of the next hop of the candidate node, which can make the right choices to send packet without the need for other network topology information, greatly reducing the consumption of maintaining network information; moreover, it has better fault tolerance and scalability, but the agreement does not take into account energy efficiency,

easily lead to excessive use of certain nodes and shorten the life cycle of the network.

Yu et al. from the UCLA University, USA, proposed GEAR (geographic and energy aware routing) routing algorithm, which combines the directional diffusion routing and GPSR routing methods, considers the node energy in the route, and thus solves the problem of unbalanced energy consumption in GEAR. GEAR assumes that the position information of the event area is known, and the nodes know their location information and residual energy. In addition, the node via a simple Hello message exchange mechanism will be able to know the location information and residual energy information for all nodes. Routing mechanism based on these address locations and energy information establish the optimal path from aggregation node to the event area to avoid flooding, reducing the overhead of route established. However, due to the lack of sufficient topology information, GEAR may reduce the routing efficiency when encounter routing void in the routing process.

5.7.3 Security Routing Protocol based on Hierarchical Structure and LEACH, TEEN Protocols

Sensor nodes are divided into multiple clusters in the hierarchical routing protocol; each cluster has a cluster head node that can not only control communication between nodes within a cluster, but also gather and fuse data of the cluster area. Then each cluster head node will send the fused data to the gateway node, which can reduce the traffic and maintain node power consumption. Typical routing protocols are LEACH and TEEN.

A research group of Professor Wendi Rabiner et al. from Massachusetts Institute of Technology proposed that LEACH (low energy adaptive clustering hierarchy) protocol is a classic clustering class routing protocol. Each round LEACH algorithm consists of establishment phase and data transmission phase of a cluster head. The algorithm allows nodes in the network balanced energy consumption and prolongs the network life cycle. But LEACH does not guarantee the position and amount of cluster heads in system, which makes the elected cluster heads distributed unevenly.

TEEN was proposed on the basis of LEACH. The basic idea is that a cluster head is selected randomly periodically and equiprobably, and the other non-cluster head nodes based on the nearest principle joined in appropriate cluster to form the virtual cluster and make energy of the whole network load evenly distributed to each sensor node, which can reduce network energy consumption and extend the network life cycle. In the process of establishing the cluster, the cluster head node broadcasts hard threshold and soft threshold to the other nodes, which can strike a reasonable balance between accuracy and data transmission network energy consumption by adjusting the two thresholds. Each round TEEN protocol consists of establishment phase and stable data transfer phase of clusters. TEEN agreement by a reasonable set of hard and soft thresholds only transmits the information of interest to users, which can effectively reduce traffic and the power consumption of the system. Simulation studies show that TEEN protocol is more effective than LEACH protocol. But like LEACH protocol, TEEN also will encounter similar Hello flood attacks, selective forwarding attacks, witch attacks, and so on.

5.7.4 Security Routing Protocol based on Multipath Transmission and SELF, MSR Protocols

Multipath routing can effectively improve the success rate of data

messages submission and balance node energy consumption to prolong the survival time of the node, while multipath routing is an effective prevention method against selective forwarding attacks.

Ouadjaout et al. proposed a new multipath routing SMRP and, on this basis, designed the SELF. In SELF, the control nodes in wireless sensor network send a key update command every one given slot. When the normal nodes receive the key update command, they will update their keys and report update result to the control nodes in their own cluster. The control nodes regard the normal nodes which have not updated their own keys in time as captive nodes and send making-invalid broadcast in the cluster. As a result, SELF can prevent the enemy from pretending to be a legal node by making use of the keys of captured sensor nodes.

Aiming at the problem of the traditional anonymous routing protocols being single path, Zhang et al. proposed a multipath protocol MPRASRP and it can effectively prevent attackers from obtaining the identity of the source node and the destination node, thereby preventing attackers from further tracking the information processing among two nodes. The method to guarantee node anonymity is that the identity of the source node and the destination node are encrypted by the destination node public key, and only the destination node can decrypt the packet. The protocol can effectively prevent the middleman attack and even under harsh environmental conditions is also very effective, but the protocol does not prevent replay attacks.

The basic idea of the MSR protocol is that, firstly, the original pieces of information are divided into subdata packets by removing code; then the subdata packets are sent out via the multiple paths. Finally, these pieces of information are combined by destination node. The agreement includes a random multipath enhanced, passive confirmation and cancellation code. Only when one need to build a random path, passive confirmation can analyze safety behavior of

neighbors based on the monitor passive traffic, reduces the routing header, has a good defense against common attacks, and thus guarantees the safety of the route.

5.8 Defense Against Attacks on WSN Routing Protocols and SPIN Protocol

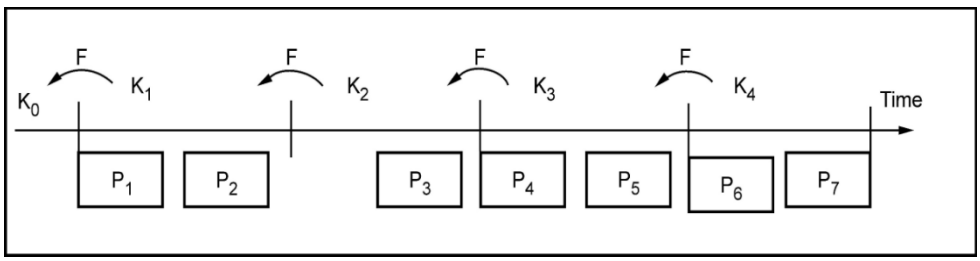
5.8.1 Defense Against Attacks on Routing Protocols

1. Many routing protocols have been proposed for WSNs. These protocols can be divided into three broad categories according to the network structure namely,
   (i) Flat structure-based routing
   (ii) Hierarchical structure-based routing
   (iii) Location-based routing
2. In flat-based routing, all nodes are typically assigned equal roles or functionality. In hierarchical-based routing, nodes play different roles in the network. In location-based routing, sensor node positions are used to route data in the network. One common location-based routing protocol is the Greedy Perimeter Stateless Routing (GPSR). It allows nodes to send packets to a region rather than a particular node. All these routing protocols are vulnerable to various types of attacks such as selective forwarding, sinkhole attack etc.
3. The goal of a secure routing protocol for a WSN is to ensure the integrity, authentication, and availability of messages. Most of the existing secure routing algorithms for WSNs are based on symmetric key cryptography, which is based on public key cryptography. μTESLA (the “micro” version of the Timed, Efficient, Streaming, Loss-tolerant Authentication protocol) and its extensions have been proposed to provide broadcast authentication for sensor networks. μTESLA is

broadcast authentication protocol which was proposed by Perrig et al. for the **security protocols for sensor networks** (SPINS) protocol. μTESLA introduces asymmetry through a delayed disclosure of symmetric keys resulting in an efficient broadcast authentication scheme. For its operation, it requires the base station and the sensor nodes to be loosely synchronized. In addition, each node must know an upper bound on the maximum synchronization error.

4. To send an authenticated packet, the base station simply computes a MAC on the packet with a key that is secret at that point of time. When a node gets a packet, it can verify that the corresponding MAC key was not yet disclosed by the base station. Because a receiving node is assured that the MAC key is known only to the base station, the receiving node is assured that no adversary could have altered the packet in transit. The node stores the packet in a buffer. At the time of key disclosure, the base station broadcasts the verification key to all its receivers.

   When a node receives the disclosed key, it can easily verify the correctness of the key. If the key is correct, the node can now use it to authenticate the packet stored in its buffer. Each MAC is a key from the key chain, generated by a public one-way function F. To generate the one-way key chain, the sender chooses the last key K_n from the



   chain, and repeatedly applies F to compute all other keys, $K_i = F(K_i+1)$.

Fig. 5.8.1 Illustration of time-released key chain for source authentication

5. The receiver node is loosely time synchronized and knows K_0 in an authenticated way. Packets P_1 and P_2 sent in interval 1 contain a MAC with a key K_1. Packet P_3 has a MAC using key K_2. If P_4, P_5, and P_6 are all lost, as well as the packet that disclosed the key K_1, the receiver cannot authenticate P_1, P_2, and P_3. In interval 4, the base station broadcasts the key K_2, which the nodes authenticate by verifying $K_0 = F(F(K_2))$, and hence know also $K_1 = F(K_2)$, so they can authenticate packets P_1, P_2 with K1, and P_3 with K_2.
6. SPINS limits the broadcasting capability to only the base station. If a node wants to broadcast authenticated data, the node has to broadcast the data through the base station. The data is first sent to the base station in an authenticated way. It is then broadcasted by the base station.
7. To bootstrap a new receiver, μTESLA depends on a point-to-point authentication mechanism in which a receiver sends a request message to the base station and the base station replies with a message containing all the necessary parameters. It may be noted that μTESLA requires the base station to unicast initial parameters to individual sensor nodes, and thus incurs a long delay to boot up a large-scale sensor network. Liu et al. propose a multi-level key chain scheme for broadcast authentication to overcome this deficiency.
8. The basic idea of this protocol is to predetermine and broadcast the initial parameters required by μTESLA instead of using unicast-based message transmission. The simplest way is to pre-distribute the μTESLA parameters with a master key during the initialization of the sensor nodes. As a result, all sensor nodes have the key chain commitments and

other necessary parameters once they are initialized, and are ready to use μTESLA as long as the staring time has passed.

9. Further there is concept of a multi-level key chain scheme, in which the higher key chains are used to authenticate the commitments of the lower-level ones. However, the multi-level key chain suffers from possible DoS attacks during commitment distribution stage. Further, none of the μTESLA or multi-level key chain schemes is scalable in terms of the number of senders. In a practical broadcast authentication protocol has been proposed to support a potentially large number of broadcast senders using μTESLA as a building block. μTESLA provides broadcast authentication for base stations, but is not suitable for local broadcast authentication. This is because μTESLA does not provide immediate authentication.

10. For every received packet, a node has to wait for one μTESLA interval to receive the MAC key used in computing the MAC for the packet. As a result, if μTESLA is used for local broadcast authentication, a message traversing l hops will take at least l μTESLA intervals to arrive at the destination.

11. In addition, a sensor node has to buffer all unverified packets. Both the latency and the storage requirements limit the scheme for authenticating infrequent messages broadcast by the base station.

12. To prevent DoS attacks, individual nodes are not allowed to broadcast to the entire network. Only the base station is allowed to broadcast, and the base station is authenticated using one-way hash function so as to prevent any possible masquerading by a malicious node. Control information pertaining to routing is authenticated by the base station in order to prevent injection of false routing data.

5.8.2 SPIN Protocol

5. SPINS is a suite of security protocols optimized for sensor networks. SPINS includes two building blocks –
   (i) Secure Network Encryption Protocol (SNEP)
   (ii) Micro version of Timed Efficient Streaming Loss-Tolerant Authentication Protocol (μTESLA)
6. SNEP provides data confidentiality, two-party data authentication, and data freshness for peer-to-peer communication (node to base station). μTESLA provides authenticated broadcast as discussed already.
7. SPINS assumes that each node is pre-distributed with a master key *K* which is shared with the base station at its time of creation. All the other keys, including a key *Kencr* for encryption, a key *Kmac* for MAC generation, and a key *Krand* for random number generation are derived from the master key using a string one- way function.
8. SPINS uses RC5 protocol for confidentiality. If *A* wants to send a message to base station *B*, the complete message *A* sends to *B* is :

$$A \_ B : D<KencrC>, MAC(Kmac, C \mid D) <KencrC>$$

In the above expression, D is the transmitted data and C is a shared counter between the sender and the receiver for the block cipher in counter mode. The counter C is incremented after each message is sent and received by the sender and the receiver respectively.

9. SNEP also provides a counter exchange protocol to synchronize the counter value in both sides.

10. SNEP provides the flowing properties,

    (i) **Semantic security** - The counter value is incremented after each message and thus the same message is encrypted differently each time.

    (ii) **Data authentication** - A receiver can be assured that the message originated from the claimed sender if the MAC verification produces positive results.

    (iii) **Replay protection** - the counter value in the MAC prevents replaying old messages by an adversary.

    (iv) **Weak freshness** - SPINS identifies two types of freshness. Weak freshness provides partial message ordering and carries no delay information. Strong freshness provides a total order on a request-response pair and allows delay estimation. IN SNEP, the counter maintains a message ordering in the receiver side and yields weak freshness. SNEP guarantees weak freshness only, since there is no guarantee to node A that a message was created by node B in response to an event in node A.

    (v) **Low communication overhead** - The counter state is kept at each endpoint and need not be sent in each message. Inspired by the work on public key cryptography, Du et al. have investigated the public key authentication problem. The use of public key cryptography eases many problems in secure routing, for example, authentication and integrity. However, before a node A uses the public key from another node B, A must verify that the public key is actually B's, that is, A must authenticate B's public key; otherwise, a man-in-the-middle attacks are possible. In general networks, public key

authentication involves a signature verification on a certificate signed by a trusted third party **Certificate Authority** (CA).

11. However, the signature verification operations are very expensive operations for sensor nodes.
12. One particular challenge to secure routing in wireless sensor networks is that it is very easy for a single node to disrupt the routing process by disrupting the route discovery process.