A Reputation-based Ant secure routing Protocol of Wireless Sensor Networks

*1 Ouyang Xi, 2 Zhang Jianyi, 3 Gong Zhe, 4 Li Qi

*1 Information Security Center, Beijing University of Posts and Telecommunications, ouyangxi@bupt.edu.cn
2, 3, 4 Information Security Center, Beijing University of Posts and Telecommunications, nese@bupt.edu.cn, gongzhe85@gmail.com, qi.liqi2001@gmail.com

Abstract

Benefit from the rapidly developing in hardware manufacturing technology and efficient software algorithms, wireless sensor networks have been widely used in many fields. Secure routing protocol in wireless sensor network has been an essential issue to consideration when security requirements are rising in deployments of sensor networks. But, in the early period, security aspects in routing protocol have not been given enough attention. So, many routing protocols of WSNs since design stage have not taken secure requirements in mind. In this paper, we proposed a secure routing protocol based on node reputation of wireless sensor network, and enlightened by the idea of ant colony optimization, the routing protocol named Reputation-based Ant secure routing protocol (RBASR). This routing protocol simulates an ant system to find the optimum route path of wireless sensor network. Distinguish from a real ant colony, RBASR use reputations of nodes as a special pheromone to evaluate rating of a path. Consider with other flexible requirements, protocol setup the optimum routing path of data transferring between the sources to the destination.

Keywords: Reputation, Ant Algorithm, Secure Routing, Wireless Sensor Network

1. Introduction

Benefit from the rapidly developing in hardware manufacturing technology and efficient software algorithms, especially, the advances in processor, memory, wireless communication technologies and information computing, the applications of wireless sensor network have been widely used in many aspects of human’s life, such as military applications, environmental monitoring, healthy care, smart home applications, and other commercial applications. But security problem is a crucial issue need to be considered when deploy an application of wireless sensor network. Many characteristics make WSNs were very vulnerable to malicious attacks. Wireless sensor network is distinguished from traditional networks, not only the constraints in sources of a node, but also lack of consideration in secure requirements during the design phase of a sensor network. Because of those particular properties, security in wireless sensor networks is more complicated.

In the following table, the main threats and vulnerabilities of wireless sensor networks were summarized and listed.

<table>
<thead>
<tr>
<th>Vulnerability</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Constrained resource(memory, battery)</td>
<td>Resource exhaustion</td>
</tr>
<tr>
<td>Low capability of computing</td>
<td>Cannot perform complicated encryption mechanism</td>
</tr>
<tr>
<td>Large number of node</td>
<td>Network congestion</td>
</tr>
<tr>
<td>Open wireless communication channel</td>
<td>Data eavesdrop and information compromise</td>
</tr>
<tr>
<td>Complicated deploy environment</td>
<td>Node physical destroy</td>
</tr>
</tbody>
</table>

The Vulnerabilities of WSNs, the harsh deploy environments and the existence of threads, requires us to put more careful security considerations into the design stage of WSNs protocols, especially, the routing protocols.

In this paper, a novel secure routing protocol of WSNs has been given which is based on the reputations of sensor nodes. The main idea of this protocol is how to set a high robustness of
communication path by using a route algorithm of node reputation, and also, this algorithm will present in following section of paper.

2. Related work

Routing protocols are the most critical components of designing and deploying wireless sensor networks, because they solve the problems of how to find a security and efficiently delivery path between a source node and destination node.

There are several well-known secure routing protocols for sensor network, such as, DD [1], LEACH [2], GEAR [3], SPINS [4], etc. To minimize network energy consumptions, data-centric routing protocol directed diffusion (DD), data aggregation and processing are required to reduce the number of transmission of redundant data. An energy-efficient communication routing protocol for wireless sensor network, low energy adaptive clustering hierarchy (LEACH), is based on nodes clustering to build up a hierarchical WSN. Sensor nodes in the local area cooperate to select a cluster head that may be more powerful so that it can perform more complex operations such as data aggregation or long distance routing. Also some routing protocols based on sensor node’s location, such as geographical and Energy-Aware Routing (GEAR). In this protocol, sensor node’s location is used as the routing metric, and it is depend by global position system (GPS) devices or any other location aware method.

But most of the routing protocols in wireless sensor networks do not consider security requirements during their design, thus most of them are vulnerable to malicious attacks. If routing protocols of WSNs fail under malicious attacks, nodes’ resource depletions, or any other vulnerabilities of WSNs, the higher layer applications will also failed and the network will become useless. So secure routing became an important area of research which is aimed to resolve those problems of wireless sensor networks.

In recent years, most researches on secure routing focus on the problem of how to improve currently existing routing protocols through plus some security mechanisms, such as encryptions, certifications and so on. For example, the majority of external attackers against sensor network routing protocols can be prevented by link-layer encryption and Authentication mechanism using a global key because attackers do not know the global key. In SPINS [4], a trustful BS can detect spoofed node identities if every node shares a unique key with it, but the centralized control may introduce too much communication or management packet overhead. Pietro et al. proposed an extension of logical key hierarchy for WSN (LKHW) [5] to protect the directed diffusion protocol. In LKHW, sink node as the root, and there is a key tree structure with source nodes, each leaf node of the tree holds keys along the path straight to the root node. The key tree is established before data are fused, then it is used to provide encryption and authentication for the data fusion. M. Tubaishat et al. proposed a Secure Routing Protocol for Sensor Networks (SRPSN) model [6], A hierarchical network is constructed with cluster heads and cluster member nodes. Messages from sensor nodes are routed by cluster heads. To protect data, a preloaded symmetric key is shared between all cluster heads and the base BS. In their approach, they divide the sensor nodes into different levels. The lower-level sensor nodes only sense and disseminate data, whereas the higher level sensors find the shortest path to the sink node and aggregate data in addition to forwarding it.

Even there are many typical routing protocols make great contributions to improve the quality in some aspects of wireless sensor networks, such as Data Delivery, Energy Efficiency, Information redundancy, etc. And in recent years, there are still many researchers focus in the field of routing of WSNs and propose novel method, such as [7]-[9]. But there is an important issue they have not considered, the security requirements. Although researchers proposed many methods to improve the security of currently existing routing protocols through plus some security mechanism, but those mechanism can not to be generally deployed in different routing protocols.

In this paper, we propose a secure routing protocol for wireless sensor networks which is based on node reputation, it is similarly to an ant colony algorithm, and the purpose of this protocol is to resolve the problem of how to find a security data transfer path between source node and destination node, so we call it Reputation-based Ant secure routing protocol (RBASR).
3. Reputation-based Ant secure routing (RBASR)

RBASR helps the sources select routing paths to the destination based not only on the shortest path but also on several secure properties of sensor node, particularly reputation of node. And we design our protocol following the idea of ant colony algorithm [10] had applied in network routing as [11]-[13].

3.1. Node reputation of wireless sensor network

Trust as a natural attribute of human society has great significance of the communicate interactions between each human social individual. A network can be considered as a microcosm of human society, trust relationships also exist between every network entities.

Reputation is quantified trust of an individual. In a reputation system, all relevant information of an individual include the behavior of itself and the recommendations from other will to be quantified, then use an appropriate computational model to evaluate trust value of the individual. Node reputation of wireless sensor network is represent node behaviors of communication whether can be trusted.

There are many researchers focus on reputation system or trust-management approach for network security. In 2001, Buchegger. S and Boudec. J. L designed a protocol named CONFIDANT [14] which is depend on the observations of neighbor nodes to identify the selfish node, and the most important issue is node reputation. Saurabh Ganeriwal and Mani B. Srivastava proposed a node reputation evaluation model--BRSN for wireless sensor network [15].

In BRSN, the reputation of node k is described as $R_k$ and $R_k \sim Beta(\alpha_k + 1, \beta_k + 1)$. Here $\alpha_k$ and $\beta_k$ represents the cooperative and non-cooperative interactions of communication of node k in observation. And the trust metric of a node is the statistical expectation of the reputation function and is given by:

$$T_k = E(R_k) = E\left[Beta(\alpha_k + 1, \beta_k + 1)\right] = \frac{\alpha_k + 1}{\alpha_k + \beta_k + 2}$$

(1)

In this paper, we use the method mentioned in BRSN to evaluate the reputation of node in WSNs.

3.2. Ant colony optimization

Ant colony optimization was originated from research the behaviors of ants searching for food. Ants use a chemical substance, the pheromone, to find the shortest path or optimal path that connects their nest to a source food. The ants deposit the pheromones while moving and tend to follow the paths with the highest intensity of pheromones. By this method, the majority of ants converge on the shortest path between their nests to the foods.

Figure 1. Ant colony shortest food path searching

In the early 1990s, ant colony optimization (ACO) [16] was proposed as a novel nature-inspired meta-heuristic for solve hard combinatorial optimization problems. By simulating the ants’ behavior of searching food, several ant based routing algorithms have been proposed. Such
as the issue of AntNet, a novel routing algorithm have been first proposed in [17] to adaptive learning of routing tables in communications network.

3.3. Processing procedure

In RBASR protocol, nodes of networks can function as source nodes, intermediate nodes, and destination nodes. Before network routing, the system firstly initials a data transfer path inquiring procedure which is described in Figure 2. When a source node wants to find an appropriate path to destination node, it sends forward inquire ants to searching for the destination.

![Figure 2. Path require procedure](image)

**Step.1 Source node initializes and send path inquire ants:**
When there is an event occurred, the source node may report it to the sink. The source node checking the neighbor nodes and sending a path inquiring ant to every node which is the next hop of itself to forward before event reporting, that is called source initialization.

**Step.2 Intermediate nodes forward inquire ants:**
When a path requiring ant reaches to an intermediate node, the ant update its information in accordance with specified rules, such as hops, reputations. Then the ant will be forward to next hop of node. Furthermore, if there is multiple next hop of this intermediate node, the ant will be copied then sends to every next hop node.

**Step.3 Destination node receives inquiring and send reply ant:**
Destination node, here is a sink node, receives all inquire ants. Potentially, the number of ants stands for the number of route between source nodes to destination node. And every ant carries the information of the path it passed. To achieve the security requirements, sink node pick up the most appropriate ant and send a reply ant backward. Other ant will be killed, and the information their taken will be kept in a reserve route information table which is store in the memory of sink node.

**Step.4 Intermediate nodes forward reply ant and update route information:**
Intermediate node receives the reply send from destination node, update its routing table according the information carried by the reply ant. Then forward the ant to the last hop. Till the last hop is the source node, the reply ant will be killed.

**Step.5 Source node receives the reply ant and setup the data transfer path:**
As the source node receives the reply ant carried optimized routing information from destination node, a data transfer path will be setup and the routing table kept in source node refreshed.

3.4. Paths require and paths enhance

We suppose there is a sensor network $W$ and with $n$ nodes between source node and destination node. We describe the connected network graph as $G = (N, P)$, and use RBASR to find the most secure path between the source node and the destination node on the graph $G$. Here variable $N$ stands for the number of nodes in graph, and $P$ represents the set of the edges connecting every pairs of neighbor nodes in graph $G$.

In RBASR, nodes choose routing path according an important parameter is the function of node reputation. We define a variable $R_{i \rightarrow j}^p$ that represents sum of nodes’ reputation on a path between node $i$ and node $j$ carried by require ant which pass the path, i.e. when an ants visit to a node is associated with an edge $e(i, j) \in P$ of the graph connecting the node $i$ and node $j$, the variable $R_{i \rightarrow j}^p$ will be modified.

The number of ants reach to the destination node represents the number of path from source to destination, also equal to the quantity of path require ants to the destination node. Figure 3 demonstrates the routes require and discovery phase in RBASR.

![Figure 3. (a)](image1)

![Figure 3. (b)](image2)
In Figure 3.(a), a source node wishing to communicate with a destination node (sink) first seeks for a route in its routing table, and finds out the neighbor nodes of next hop in its routing table. This is a source node initialized routing discovery phase, and the messages called require ants of route-request have been broadcasted. In this case, there are several potential paths connected source with destination, but only the optimum path according to the information carried by related ants should be picked up by destination. Then the destination replies a corresponding backward ant (route-reply message) backtrack to the source, after source receives the reply and updates the route information table, the data transfer tunnel setup as shown in Figure 3.(b) and Figure 3.(c).

### 3.4.1 Rules (or principle) of sending require ants

a. Only send to the neighbor nodes of it;

b. Should not send to the neighbor which is last hop in routing table of itself?

c. If a node requires above requirements but it is the last hop of another node which requires above requirements too, it should not to be an objective that is source node sends ant to.

### 3.4.2 The optimum path in graph

$N_p$ is the set of intermediate nodes of a path connect source to destination. When an ant passed node $k \in N_p$ which is the intermediate node between source node $i$ and destination node $j$ records the reputation of the node $k$: $R_k$ and add it into $R_{s \rightarrow d}^p$. When a require ant arrives to destination, the result of $R_{s \rightarrow d}^p$ follows:

$$R_{s \rightarrow d}^p = \sum_{k \in N_p} R_k$$

(2)

An accumulator $H_{s \rightarrow d}^p$ represents the hops of path carried by a require ant. When the ant passes through an intermediate node, the accumulator counts one. In the network graph $G = (N, P)$, the hops number of max hop path is represented as:

$$H = \max \left\{ H_{s \rightarrow d}^p, P \in G \right\}$$

(3)

For each path, a definition $R_p$ denotes the minimum reputation value of node which is connected by the path. As follow:

$$R_p = \min \left\{ R_k, k \in N_p \right\}$$

(4)

Compare with traditional routing methods, RBASR put an additional time into routing discovery phase. Suppose a require ant takes a time of delay, described as $\Delta t$, on every edge connected two neighbor nodes. And the treatment time of routing decision on destination assumed to be a constant $\lambda$. 
All the information mentioned above of a route path is carried by a related require ant. In the destination, every potential route path will be evaluated and be given rating cores according the formula as follow (\(\alpha\) and \(\beta\) represent weight):

\[
\text{PathRating} = \left\{ \alpha \left( \frac{R^p_{S\rightarrow d}}{H^p_{S\rightarrow d}} \right) + \beta \left( 1 - \frac{H^p_{S\rightarrow d} \cdot \Delta t}{H \cdot \Delta t + \lambda} \right) \right\}, \quad \alpha + \beta = 1
\]  

(5)

The highest rating path is considered as the optimum path between the source to the destination in graph. In the path evaluate and choose phase, protocol also allow add some additional requirements for fit special conditions. In the most general case is declares an acceptable lowest value of minimum reputation value of node.

4. Simulation and analysis

In this section, we deploy a simulated environment of RBASR with OPNET [18] as shown in the Figure 4. In this case, we suppose there are 100 sensor nodes with one sink node in a wireless sensor network. Events are randomly happened in the monitor field of network, and there is only one destination that is the sink node. In other words, whatever which sensor node monitored an event happen, the information always deliver to the sink node finally.

To simulate more closely to a real network, because wireless sensor network always deployed in severe environment, we set many malicious sensor nodes randomly in the monitor field. When a malicious node receive a date package requires forward, the most happened is the package loss.

![Figure 4. Simulated deployment in OPNET](image)

We focus the robustness of the routing protocol first, because the goal of secure routing is find a path of data delivery is safety enough. To get a directly impression of the performance of RBASR, we compare it with a popular sensor network routing protocol—Directed Diffusion (DD) [1].
The results of simulation implicated that the data delivery ratio of RBASR and DD slightly decreases for larger distance (hops) from the source to the sink. But the delivery ratio of DD drops much faster than RBASR for any source-destination hops. RBASR perform higher robustness of data delivery. Because by the method of RBASR pick up the nodes build up a path of data delivery, malicious nodes are avoided as far as possible. Figure 5 illustrates the data delivery ratios of different distance from the source to the sink.

Figure 6 reports the comparison of delay in different routing protocol with same path length. And the results show that the delay of RBASR is more than DD in a short path, but the performance in RBASR is better than DD during path length increased.

5. Conclusion

In this paper, we proposed a novel routing protocol based on node reputation of wireless sensor network enlighten by ant colony optimization—Reputation-based Ant secure routing protocol (RBASR). Simulate the behaviors of real ants searching for food, RBASR send route require ants from the source to the destination. RBASR collect information of every potential path by ants and use a special pheromone—reputation of node to evaluate the rating of a path. By this method, the optimum path between the source to the destination will find out and finally setup to deliver data. We setup a simulated environment to analyze the performance of the protocol, and compare with other typical routing protocol of WSNs, the results show that RBASR has a better performance on safety data delivery.

6. Acknowledgements

This work is supported by the Key Project of Chinese Ministry of Education China Postdoctoral Science Foundation funded project (20100471762), National S&T Major Program (2011ZX03002-005-01) and National Natural Science Foundation of China (No. 61121061).

7. References