Secure Data-Centric Routing Protocols in categorized WSN Using Proficient KDS

K. Rajasekaran¹, Dr. Kannan Balasubramanian²

¹Department of Computer Science, Manonmaniam Sundaranar University, Tamilnadu, India, raja21raja@yahoo.com
²Department of Computer Science, Mepco Schlenk Engineering College, Tamilnadu, India, kannanbala@mepcoeng.ac.in

Abstract- Recent advances in wireless sensor networks have led to many new protocols specifically designed for sensor networks where energy awareness is an essential consideration. In this paper an efficient key distribution scheme used to secure data centric routing protocols WSNs. Like these routing protocols, single-handedly proposed scheme secure key distribution with a centralized process that gives a multilevel hierarchical organization for wireless sensor networks. The originality of this work is to allow local use of key distribution process to establish group key pairs and Key. These two kinds of keys are useful for respectively setting data request broadcasting and transmission of data over multiple hop routing paths. Moreover, when WSN topology changes, the proposed scheme enables secure WSN reorganization. The analysis explains that our proposed scheme can support various possible attacks on wireless sensor networks.

Key words— Wireless sensor networks; secure routing key distribution scheme; data-centric routing protocol

I. INTRODUCTION

Recent advances in micro-electro-mechanical systems and low-power, highly integrated digital electronics have led to the development of micro-sensors. Such sensors are generally equipped with data processing and communication capabilities. The sensing circuitry measures ambient condition related to the environment surrounding the sensor and transforms them into an electric signal. The detection circuitry measures ambient conditions related to the surrounding environment sensor and transformed into an electrical signal. Processing such a signal reveals some properties of the objects located and/or events occurring in the proximity of the sensor. The sensor sends this data collected, usually by radio transmitter; to a command center (sink) directly or through a data concentration center (a gateway). The decrease in the size and cost of sensors, as a result of the developments, has fueled interest in the possible use of large set of disposable unattended sensors. Such interest has motivated intensive research in the past few years to address the potential for collaboration between sensors in data collection and processing and coordination and management activity detection and data flow to the sink. A native distributed architecture such collaboration sensor network is a wireless link that can form between the sensors of an ad hoc fashion. When the routing protocol is compromised, there are fatal consequences in the operation of sensor networks, such as limited availability, the deviation of the data, the energy dissipation and network disruption. Such interest has motivated intensive research in the past few years addressing the
potential of collaboration among sensors in data gathering and processing and the coordination and management of the sensing activity and data flow to the sink. A natural architecture for such collaborative distributed sensors is a network with wireless links that can be formed among the sensors in an ad hoc manner. Networking unattended sensor nodes are expected to have significant impact on the efficiency of many military and civil applications such as combat field surveillance, security and disaster management. These systems process data gathered from multiple sensors to monitor events in an area of interest. For example, in a disaster management setup, a large number of sensors can be dropped by a helicopter. Networking these sensors can assist rescue operations by locating survivors, identifying risky areas and making the rescue crew more aware of the overall situation. Such application of sensor networks not only can increase the efficiency of rescue operations but also ensure the safety of the rescue crew. On the military side, applications of sensor networks are numerous. For example, the use of networked set of sensors can limit the need for personnel involvement in the usually dangerous reconnaissance missions. In addition, sensor networks can enable a more civic use of landmines by making them remotely controllable and target specific in order to prevent harming civilians and animals. Security applications of sensor networks include intrusion detection and criminal hunting. Security services for routing protocols based on symmetric cryptographic algorithms that require key distribution mechanisms. The studied routing protocols are bootstrapped with a centralized process and provide a hierarchical organization to the WSN [1][2][3][4][5]. It is recommended that the proposed system of key distribution should be readily attached to the security protocols of data-centric routing. Must be able to efficiently share three types of keys: Global Key, Group Key, Pair wise key and to ensure different communication patterns: one for all, one too many and one to one. Furthermore, the proposed system must allow safe WSN reorganization.

II. Related Work

Centric routing protocol data is not based on the address data but rather sensors. Initially, the base station transmits a "request for data" message. Sensor node that receives this message again proceeds to broadcast to all neighbors. After a period of time, "data request" messages reach the entire network. If a sensor node has data to satisfy the request, it sends a "Response data" message through the best gradient (router). Data centric routing protocols allow in-network processing (eliminating redundant data, aggregation). It results in a reduction subsequently send a reduction potential collisions in the transmission channel. These aspects lead to energy savings and increase the lifetime of the network. For interest next, "Application data" message can be sent to a multicast group nodes or uni-cast to a specific node. Below, we give more details on the data centric routing protocols. For Directed Diffusion, “Data Request” message represents an interest to data. Messages of support Interesting name attributes that specify a set of constraints that must be met sensing data to sink node waits, as the data class. You can specify other parameters, such as the expiration of interest rate and shipping. Thereafter, nodes with data corresponding to these limitations send data through all gradients. Whereas for One Phase Pull –a lightweight variant of Directed Diffusion– data messages are sent back along the fastest gradient from which the first interest message was received. In Flooding and Gossiping “Data Response” messages are sent randomly among one of
the gradients. This allows load balancing and avoids having famous nodes. Whereas, for Energy aware routing, routing metric is a function of consumed energy throughout the routing path. For gradient based routing, sensor nodes keep the number of hops when the “Data Request” message is diffused through the network. Therefore, each node can detect the minimum number of hops to the sink height is called the node. Thus, the "response data" messages are sent through the routing path with minimum gradients.

On the other hand, different key distribution schemes for WSNs are proposed in literature [6][7]:
- Public key schemes: with limited resources, sensor nodes cannot employ sophisticated public key cryptographs. Though, some work on ECC promises easy key management but this is for heterogeneous WSNs where routers dispose most capabilities [8].
- Single network-wide key: a single key is preloaded into all nodes of the network. For example, Tinysec [9] proceeds with a single network-wide key along deployment phase. The main drawback is that the compromise of a single node causes the compromise of the entire network.
- Complete Pair wise Key sharing: for a network of n nodes, (n-1) Pair wise keys are retained in each node’s memory. This approach is not scalable.
- Random key pre-distribution scheme: in this scheme, a pool of keys is initially pre-loaded into each sensor. After this, sensor nodes undergo a distributed discovery process to set up shared key for secure communications [10]. This scheme isn’t convenient to a centralized bootstrapping communication. Also it doesn’t ensure that two nodes are always able to compute a Pair wise Key.
- Hierarchical key management: it supports various secure communication patterns: unicast, multicast and global broadcast.

LEAP+ [11] is referred to as the basic scheme of hierarchical key management. LEAP+ initially establishes Pair wise Key with a distributed process. This isn’t the case of the above routing protocols where communication is bootstrapped with a centralized process.

- Key Distribution Center: in this scheme [12], base station sends a session key to secure communication between any two nodes. The scheme has small memory requirement. It is resilient to node capture and possible to revoke key pairs. The main drawback of this scheme is not scalable.

III. PROPOSED SYSTEM

Considering the particularity of routing in wireless sensor networks where "response data" messages are sent mainly to the base station, thus "data request" messages received from nodes with greater height (farther from the station base) will be rejected. In fact, for the Directed Diffusion and Phase One Tire a message of interest received from gradient data is interrupted. Energy-aware routing protocol, the routing path containing nodes subordinate is obviously more expensive in terms of energy expended. Flood & gossip and gradient-based routing, "response data" messages are sent to the base station. Consequently subordinate nodes must not belong to the routing paths. Also in MTE [13], it is shown that sending via an intermediate node induced less dissipated energy than a direct communication. As a result, in the proposed key distribution scheme, each sensor node will seek to share Pairwisekey with nodes (routers) having little or equal height. Thereafter, the routing metric to determine the best gradient. Moreover, the hierarchical organization offered by the WSN routing protocols is dedicated to establishing group key for each group of nodes. More precisely,
the proposed system key distribution with the following objectives:
To make sure a hierarchical organization of the WSN:
• Establish group key and key pairs,
• Promote low overhead storage, computation and communication
• To allow the WSN reorganization sure and allow key refresh.

To achieve these objectives, the key distribution scheme that takes into account some features:
• Routing protocols studied using a centralized process (initiated by the base station) to organize WSN, then the key distribution process will proceed in the same manner, to give a certain organization.
• The first issue will be password protected Global preloaded.
• The process of establishing and Pairwisekey group key should be performed locally,

The key distribution scheme requires two steps to perform these functions. Table 1 show the notations used in this description.

<table>
<thead>
<tr>
<th>Notation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BS</td>
<td>Base Station</td>
</tr>
<tr>
<td>N</td>
<td>Sensor Node</td>
</tr>
<tr>
<td>GH</td>
<td>Group Head</td>
</tr>
<tr>
<td></td>
<td>Broadcast address</td>
</tr>
<tr>
<td>A</td>
<td>Data A concatenated with data B</td>
</tr>
<tr>
<td>MACK(A)</td>
<td>MAC calculated and encrypted with a key K</td>
</tr>
<tr>
<td>Enckey(A)</td>
<td>Encrypt data A with a key K</td>
</tr>
</tbody>
</table>

Table 1. Notations table

1. Group Key Distribution

Each node is preloaded with a global key. As WSN is deployed, the proceeds from the base station of a secure issuance of a "Discovery Path" message to trace the routing paths. Finally, this message is used to distribute group key. To easily determine the node level, a height field is added to the message. The height value received in the message determines the level of the first node.

BS = *: * || BS ||Nonce|| height || EncGlobalKey (Group Key) || MACGlobalKey

Each node N receive secure "Path Discovery", this message is retransmitted. When the "Discovery Path" dissemination is achieved, the WSN is organized into hierarchical groups safely. More precisely, the intermediate nodes are group head, each node N belongs to one or more groups who share a group key. Finally, each sensor node deletes the key memory Global preloaded.

The use of the Global Key is well limited in time. This reduces the impact of a tamper attack only to links with immediate neighbours and not to the entire network. It is important to say that the broadcast duration for various sizes must be taken into account. It shouldn’t exceed the necessary minimum time so that an attacker reveals information stored in a sensor. Studies carried out in [14] showed that it takes at least 10 seconds to tamper a captured node. Since, several techniques were proposed to protect sensors against tampering. But tamper-proof sensor nodes are more expensive. Recalling that the key distribution scheme is proposed for homogeneous WSNs, keep 10 seconds as the minimum time required for disclosure of a regular sensor node.

2. Pair Wise Key Distribution

At the end of "Discovery Path" broadcast, a node N sends a secure message "Join Group Request" to the heads of their group. Over time, this post will be useful to share with each of them a pair wise key.

N = GH: GH || N ||Nonce|| Enc Group Key (Pairwisekey) || MACGlobalKey Therefore, for each entry in the "group box Head" an N node precedes. When a "Join Group Request" message is received by a group leader, proceed as shown in The "Join Group
Response" message is sent to a group member node N to confirm secure link:
\[ GH = N \ || \ GH \ || \ Nonce\| \ MACPairwiseKey \]
When phase 2 is reached, the actions of a node n key pairs with each group leader (candidate router). After that, the routing protocol determines the best gradient (router) to the base station.

3. Secure Deployment of Routing Protocols

Once the two previous phases are completed, the WSN is organized with a secure process that provides each node candidates secure link with routers. Thus, for any routing protocol studied, the base station can initiate the creation of secure routing path for disseminating "information request" message that is password protected group. Furthermore, intermediate nodes proceed the same way, until the leaf nodes of the network are reached. Consequently, each node has significant data, be able to send secure "response data", protected key pairs, through the best gradient.

4. Secure WSN Reorganization

When the base station expresses a need for new data, the first phase of routing protocol consist of a secure broadcast "data request" message. This allows the safe reorganization WSN therefore a trace routes the secure multi-hop routing.

5. Key Refresh

To maintain security in wireless sensor networks, shared keys must be efficiently cooled with the local process. Therefore, a group leader may redistribute a group key with the multicast message. In addition, a node can refresh group member key pairs with Group Leader. Key messages of soda can be password protected sharing. Additionally, when a sensor node is compromised or leaving the WSN, an organization committed node deletes keys shared with him. Therefore, a group leader in question starts a local redistribution Key Group each member protected by pair wise key.

IV. SECURITY ANALYSIS

In this section, we analyze the immunity of key distribution system against known attacks of wireless sensor networks. The data rate lock: the key distribution system initiates communication by spreading the "discovery path" message. This makes it difficult for an adversary to prevent the arrival of the messages to sensor nodes.

- Physical attacks: In the hostile environment, some sensor nodes can be caught and handled. Obviously, the most sensitive information is shared keys. The impact of these attacks affects only secure links with its immediate neighbors and not the entire network.
- Replay attack: if an attacker tries to play old messages, this is because each node stores the last nonce.
- Black Hole: if an attacker with high capacity communication relays a message, you cannot create a black hole in the WSN because it cannot be authenticated by the sensor nodes.
- Sybil attack: even if an attacker has multiple identities, this is not because you cannot authenticate.
- Flooding attack: this attack does not hold because the message is not authenticated are discarded.
- Brute-force attack: the insurance plan allows refreshing key distribution group key and key pairs that limit the effect of this attack.
V. ANALYSIS OF ROUTING PROTOCOLS

In literatures, other key pre-distribution schemes have been proposed for securing WSNs having similar organization. SNEP is a KDC based on key pre-distribution scheme. Before deployment, each node is preloaded with a symmetric key shared between itself and the base station. If two nodes want to share a key pair comparison, it is essential that communicate with the base station establishes a pairwise key for them. If the WSN uses multi-hop routing paths, SNEP cause a high communication overhead. To reduce such required channel capacities a solution, in [15] consisting in incorporating SNEP in the routing protocol. As a result, the message size is increased. This is not effective because Pairwise Key update is not required in each dissemination.

In the work SecOPP [16], proposes a secure version of One Phase Pull protocol where the key distribution scheme is incorporated in the routing protocol. As a result, the length of the routing message for subscription increases alongside data. Moreover, regarding routing protocols provide a gradient only when a secure link between a source node and its gradient are lost, the source node cannot join the network during the reorganization is sure. Consequently, the source nodes of the network will be isolated and the nodes that are connected to them. To overcome this problem, the current protocol key distribution enables each node to share keys with multiple routers that have little or equal height.

To check functionalities of the proposed key distribution scheme, simulations are made with NS2. Sensor nodes are deployed in a random greed. The base station is located in the upper left corner. The signal range is approximately 10 feet. A radio model used with NS2. Initially, we tested routing protocols to be protected with a different network size. To ensure that the detected data arrives at the base station, we tested a lightweight centric protocol routing data as a diffusion phase extraction. Figureure1 shows the initialization of efficient key distribution scheme after doing 3 tests for each network size, we noted that when the sensor nodes number exceeds 90, diffusion of “Data Request” messages does not reach certain leaf nodes. They will be considered as orphan nodes. The topology obtained when a pull phase implemented in a WSN has 30 sensor nodes. Therefore, we will be happy to secure these routing protocols for networks with less than 100 nodes and the path discovery between the group’s keys within the transmission range. The authentication of group wise key is used for the security purpose and the authentication of pair wise key generated is used to pair key within group wise keys. We have calculated necessary time so that the key distribution scheme achieves Group key and Pairwise key distribution. Remembering at the end of Group Key distribution, Global Key is removed from all sensor nodes. Figure. 1&2 shows the required time for different network size.

6. SIMULATION AND EXPERIMENTS RESULTS
Performance of Pair wise Key Distribution

Figure: 1 Performance of Group key Distribution

Performance of Group Key Distribution

Figure: 2 Performance of Group key and Pair wise key Distribution

Figure: 3 One KDC compared to the proposed Scheme

The curve which presents the necessary time to distribute Group Key shows well that Global Key can be removed before deployment time reaches 10 seconds. Indeed, for a WSN which contains 90 nodes the Global Key is removed from each sensor before 9 seconds. To check contributions of the proposed key distribution scheme carried out in the earlier works based on the use of one KDC are simulated with the same platform. The Figure. 3 present a comparison in terms of necessary time. The curves of the proposed key distribution scheme are well placed at the lower part. The effectiveness of our scheme is more visible when the number of nodes increases. This explains its scalability.

7. CONCLUSION

Our secure solution gives an efficient key distribution scheme to the studied data-centric routing protocols. It provides local process to share Group Key and Pairwise Key in hierarchical WSNs. Furthermore, it allows secure WSN reorganization. Security analysis explain that it can withstand several attacks against WSNs. Simulations illustrate that it is scalable and more efficient than earlier works which are based on One KDC. All these show that our proposed key distribution scheme is suitable to secure the studied data-centric routing protocols. In the future, we will provide a formal proof of security properties for the proposed scheme. In addition, we will demonstrate all these results with analytical study.

REFERENCES


