A Secure Routing Method on Wireless Mesh Sensor Networks (WMSNs)

Mohsen Imani, Hamid Reza Tavakoli, Mohammad Ebrahim Rajabi, and M. Naderi

***Abstract*—Wireless sensor networks (WSNs) are based on the random deployment of a large number of tiny sensor nodes and actuators into or very close to the phenomenon to be observed. These networks face with several essential challenges; for example, power consumption and secure routing are critical problems in the wireless sensor networks. To reduce power consumption, this paper proposes an efficient architecture with optimal power management for WSNs. This architecture merges wireless sensor network into wireless mesh networks. The other aspect considered in this paper is the secure routing in the new scheme of wireless mesh sensor network. This paper presents a secure routing algorithm for the proposed wireless mesh sensor network.**

***Index Terms*—Component, sensor networks, mesh networks, power consumption, secure routing, wireless mesh sensor network.**

I. Introduction

With the advent of wireless communications, different applications in wireless networks have been performed in portable devices (e.g., cellular phone, PDA, lap-top, etc.) or wireless sensors (e.g., CCD camera, cordless speaker, optical detector, etc.). In the wireless sensor networks (WSNs), each of wireless sensors can exchange mutual data or forward other traffic flows by using the wireless routing protocols [1]. The sensors will consume more power in forwarding packets in the WSNs. One of the most important issues in the WSNs is routing. The routing in the WSNs is considered from various points such as the security and the power consumption [2].

Research on the sensor network routing focused on efficiency and effectiveness of data dissemination. Few of them considered security issues during the design time of a routing protocol [3]. A number of routing protocols have been proposed for sensor networks, such as Directed Diffusion [4] and LEACH [5]. However, these routing protocols for the WSNs are built on the network architecture (called flat architecture) such that all sensor nodes are homogeneous and send their data to a single sink node by multiple hops and the network is considered as single routing domain [6], [7]. Flat algorithms have several drawbacks such as unbalance on energy consumption, poor scalability, poor robustness, and single point of failure [8]. These shortcomings forced the researcher to change their ideas about the routing algorithms. The other routing algorithm is Hierarchical-Topology Algorithm. In these algorithms, nodes are grouped into clusters and one node in each cluster is selected as cluster-head that it manages the cluster and forwards packets originated from the cluster nodes toward the access point [9].

The wireless mesh sensor networks which are a combination of the wireless mesh and sensor networks can also be considered as a kind of the hierarchical algorithms. By deploying some super mesh nodes with capacities to transmit data in a long-distance way and self-organize reliably, the WMSNs merge the advantages of wireless mesh networks and wireless sensor networks. The WMSNs do not have a well-defined architectural model with scalability and robustness. Also, there is a lack of secure and energy-efficient routing protocols for the WMSNs at this time [8]. Thus, this paper presents a new architecture of the WMSNs and considers it from the point of view of secure routing. In the proposed method, it is assumed that the mesh nodes (gateways and mesh routers) are deployed in the sensor networks. The gateways are periodically able to move where-ever into the sensor networks. Every period during is called a *round.* The sensor nodes are connected to the mesh nodes to communicate with the access points.

The rest of the paper is dedicated as follows: a description of the wireless mesh sensor networks is provided in Section II. This section explains the wireless mesh networks and the proposed architecture. In Section III, the proposed secure routing algorithm and necessary assumptions in the new architecture is described. Eventually, the mobility of the gateways into the sensor networks is considered in Section IV.

II. Wireless Mesh Sensor Networks (WMSNs)

In this section, the proposed architecture of the wireless mesh sensor network is presented. At first it is tried to explain a wireless mesh network briefly. Then, the wireless mesh sensor network, as a network which it merges the advantages of both of the wireless mesh and sensor network, is presented and its most important issues are considered.

A. Wireless Mesh Networks

The wireless mesh networks are a new paradigm of the wireless networks which are very noteworthy at the present. These networks are able to cover a vast area by low power consumption and can also integrate with other wireless networks, such as cellular, sensor, and local area networks.

The nodes in WMNs are two types: mesh clients and mesh routers. The mesh clients and routers have several differences in the mobility, the power computation, the gateway and bridge functionalities, the energy limitation, and the storage space. The mesh routers make backbone of

Manuscript received September 9, 2014; revised November 13, 2014.

The authors are with School of Electrical Engineering, Iran University of Science and Technology, Tehran, Iran (e-mail: moh.imani@ieee.org, tavakoli@iust.ac.ir, merajabi@elec.iust.ac.ir, m_naderi@iust.ac.ir).

the WMNs, and so, the WMNs are able to connect to the other networks by means of these nodes [10]. An example of the wireless mesh network has been shown in Fig. 1.

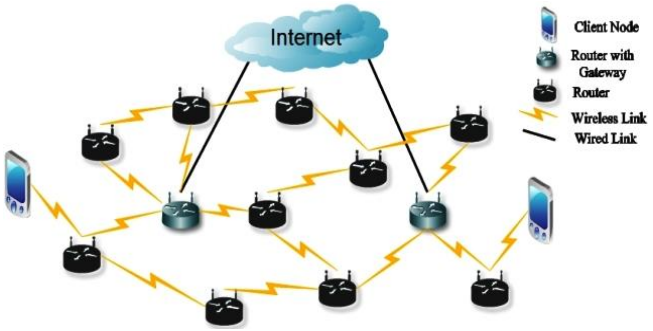

Fig. 1. An example of the wireless mesh networks.

B. The Proposed Architecture

In traditional wireless sensor networks, there is single sink node that energy of the nodes around it is drained sooner than the other nodes. This leads to decrease the network lifetime. From the point of view of security, if the nodes near the sink are compromised, it actually makes a disturbance in thr performance and security of the network [8]. In this case, it is proposed to apply multiple sinks into the network. This means that a wireless mesh network has to be implemented throughout the sensor network. The gateways of the mesh network are deployed throughout the sensor networks and make an infrastructure for the sensor networks.

Indeed, the combination of the wireless sensor and mesh network forms a wireless mesh sensor network and it has the advantages of both of them. The wireless mesh sensor network includes three sub-level networks which are as follows:

- *Wireless Sensor Network*: it consists of spatially distributed autonomous sensors to cooperatively monitor physical or environmental conditions, such as temperature, sound, vibration, pressure, motion or pollutants and it is lower sub-level network.
- *Wireless mesh network*: it consists of the mesh routers and gateways and connects the lower sub-level to higher sub-level. It is the middle sub-level network.
- *Internet*: it makes access to sensed data remotely. It is the high sub-level network.

This proposed architecture of wireless sensor network has three types of node:

- *Wireless Mesh Gateways (WMGs)*: these nodes work as sinks for lower sub-level sensor network, as well as the routers of the middle sub-level mesh network.
- *Wireless Mesh Routers (WMRs)*: these nodes have just the router role in the middle sub-level mesh network.
- *Sensor nodes*: these nodes gather the environmental data.

In this architecture, the sensor nodes gather the environmental data from the area where they are deployed and send them to the WMGs. The data are routed by the WMGs and WMRs to the access points (APs). By using the WMGs deployed throughout the sensor network, the average numbers of hops of data transmission are decreased and this accordingly leads to lengthen network lifetime. However, the sensor nodes near the WMGs still drain their energy sooner than the other nodes because of forwarding their packets. On the other hand, the most important point in this case is the model of the gateways deployment. Gateway deployment model describes how to distribute WMRs and WMG based on location and scheduling in a specified sensor network.

For solving above issues, it is assumed that the WMGs enable to move and change their location in the sensor network. Because of decreasing the overhead in finding a route to WMGs in the sensor network, it is considered that the WMGs move in the sensor network periodically. The WMGs stay in the specified locations in a period. After that, for balancing energy among the sensor nodes and security issues like detection of gateways location, the WMGs move and change their locations. The WMGs inform the sensor node from their location change with a Notification placket. The Notification packet and mechanism of the changing location are described in the subsequent section. Note that the movement of the WMGs is under the area where covered by sensor network and the WMGs have to be within radio range of the other WMGs and WMRs.

As mentioned above, the functionality of the WMSNs can be explained as follows. All of the mesh nodes form a backbone in the network. The powerful mesh nodes have more energy supply, longer transmission range, higher data rate than sensor node, and they provide many advantages for designing better secure routing protocols. The basic idea of routing in the WMSNs is to let each sensor node sends data to a WMG. A WMG can aggregate data from multiple sensor nodes, remove redundant data, and send the compressed data to the APs via the mesh backbone [9]. Transmissions in the backbone can use a different frequency and have longer range than transmissions among sensor nodes. Based on the two-tier communication architecture, the routing in the WMSN consists of two parts: routing between the lower sub-level sensor network and the middle sub-level mesh network and the routing between the middle sub-level mesh network and the higher sub-level Internet. An example of the wireless mesh sensor networks has been shown in Fig. 2.

III. The Secure Routing in the Proposed Architecture

The routing is an essential operation in the sensor networks. The routing in a network includes finding a route for transmitting data between two nodes. The most protocols do not consider security necessities. This section presents a new method for the routing in the proposed architecture.

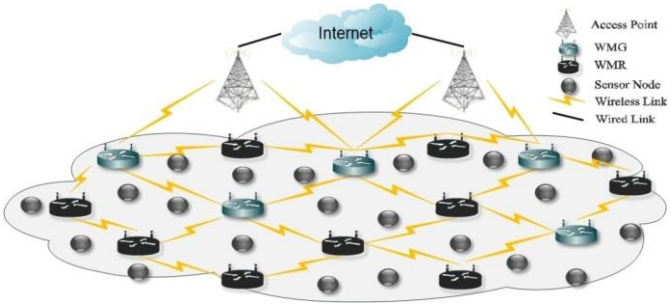

Fig. 2. Example of a wireless mesh sensor network (WMSN).

In the architecture discussed above, the mesh network

routing in middle layer has been well researched. This Section focuses on the routing in the lower sub-level sensor networks.

A. Principles and Assumptions of the Routing in WMSNs

In this paper, the best route is a route which has minimum hops to a WMG. Thus, the shorter route, the less energy consumption. It leads to a long lifetime for network. In this paper, it is assumed that the WMRs and the sensor nodes are static but the WMGs can move in the sensor network. Note that the movement of the WMGs is not continuous and they move periodically. Each period during which all gateways are static called a *round*. As a result, during a *round*, the sensor network topology keeps fixed.

When a sensor node finds the shortest route to the WMGs in a *round* it does not need to find the route to the WMGs for transmitting data during the *round*. In this method, a serial number is defined for each *round*. When a WMG wants to move, it broadcasts a Notification packet which is signed by a private key. This notification packet includes the serial number of the *round*.

For describing the routing algorithm in the proposed architecture of the WMSNs, *m* gateways are considered to be deployed in a sensor network. In this network, the mesh nodes (WMGs and WMRs) are trusted. Each sensor node includes a routing table with *m* entries.

In order to evaluate the routing algorithm from the point of view of security, three keys are defined. These keys are as follows:

- K: a secret shared key among all nodes of the network (including WMR, WMG, and sensor node).
- K_i: a symmetric secret shared key between a specified sensor node S_i and all of the gateways and the routers (WMGs and WMRs).
- K_p: it is a private key which is available to all of the WMRs and the WMRs. The public key of this asymmetric cryptography is available to all of the nodes of the network. All mesh nodes have the private key.

B. Secure Routing Algorithm for WMSNs

When the sensor node S_0 needs to send its data to the APs, it checks its routing table to find a fresh route to the WMGs. the fresh route should be within a *round* with valid serial number. If it cannot find a fresh route to a WMG, it generates and broadcasts a route request (RREQ) message throughout the network. This message includes the following information: message type (rreq), source id (S_0), message number ($S_0\#$), the destination which it is set to G to show all of the gateways are intended, and a MAC (M_{S_0}) computed over these elements with the shared key K_0. In this message, $S_0\#$ is nonce, randomly generated number, to uniquely identify each RREQ generated. The M_{S_0} is used by the mesh nodes to verify the authenticity and freshness the RREQ generated. This message also includes a path list which is used for appending the intermediate nodes and it is encrypted by the secret shared key among all nodes of the network (K). All parts of the RREQ are as follows:

$$msg_{rreq} = \{rreq, S_0, G, S_0\#, M_{S_0}, (( ), G_1, G_2, \dots, G_m)_K\} \quad (1)$$

where $(( ), G_1, G_2, \dots, G_m)_K$ is the path list. At the end of the path list, the source node lies all of the gateways of the network. This is used by the intermediate nodes for replying to the RREQ if they have a fresh route to a specific WMG.

When an intermediate node received a RREQ, it checks its routing table to verify if it has a fresh route to the gateways. At first, it is considered that the intermediate node S_i has a fresh route to the gateway G_2. Then it applies three changes on the RREQ. It firstly removes G_2 from the path list and then appends itself to it. Finally, it computes a MAC value on the following parts with K_i and then replaces it with $M_{S_0 S_1 \dots S_{i-1}}$. This MAC value protects the RREQ message from the route falsification attacks and prohibits the intermediate nodes to remove the nodes of the path list to show a shorter path.

$$M_{S_0 S_1 \dots S_i} = MAC_{K_i}\{rreq, S_0, \mathrm{G}, S_0\#, M_{S_0 S_1 \dots S_{i-1}}\} \quad (2)$$

After all, the sensor node S_i broadcasts the message. This message has a form as follows:

$$\{\mathrm{rreq}, S_0, \mathrm{G}, S_0\#, M_{S_0 S_1 \dots S_i}, ((S_1, S_2, \dots, S_{\mathrm{i}}), G_1, G_3, \dots, G_m)_K\} \quad (3)$$

When a gateway G_j receives a RREQ, it waits for a while to receive other RREQs. After that, it computes the shortest route among routes of the received RREQ messages. The shortest route has the minimum hops. it verifies the MAC value in the RREQ for authentication of the source and integrity of the path list. Also, the WMG checks the message number ($S_0\#$) for detecting the replayed message from a malicious node. Therefore, If these verifications are correct, the gateway G_j appends itself and the serial number of *round* ($\mathrm{N_r}$) at the end of the path list and then sings it by K_p because it can show this path is approved by a legal gateway.

Finally, the gateway G_j creates a route reply message (RREP) which it includes the following items: message type (rrep), S_0, G_{j}, $S_0\#$, a MAC ($M_{\mathrm{S_0},G_j} = MAC_{K_0}\{rreq, S_0, G, S_0\#, G_j\#\}$), and the path list. The MAC value is used by the source to verify the authenticity and the freshness of the RREP generated.

Note that in the path list the gateway G_j only appends itself at the end of the path list because this informs the intermediate nodes that it is a route to the gateway G_j. The serial number (N_r) into path list informs the intermediate nodes that it is not a replayed message from the previous *round*s. A typical RREP message is as follows:

$$msg_{rrep} = \{rrep, S_0, \mathrm{G_j}, S_0\#, \mathrm{M_{S_0,G_j}}, \left(S_1, S_2, \dots, G_{\mathrm{j}}, N_r\right)_{K_p}\} \quad (4)$$

When a sensor node receives a RREP, it checks the path list in the message; if it finds its id in the path list, it forwards the RREP message in terms of information in the path list. It also records the path list along with the signature in its routing table.

Let's consider a case in which a intermediate sensor node S_i has received a RREQ and it has a route to G_j. This algorithm let it reply to the source sensor node. For doing it, the sensor node $\mathrm{S_i}$ computes $M_{S_0 S_1 \dots S_i}$ and appends itself to

the path list, it also has to append its received signed path list from gateway G_j. After that the sensor node S_i changes "rreq" to "rrep" and changes G to G_j into the received RREQ and forwards it to the previous node. This message is as follows:

$$msg_{rreq} = \{\, \text{rrep}, S_0, G_j, S_0\#, M_{S_0 S_1 \ldots S_i}, (S_1, S_2, \ldots, S_i), (S_{i+1}, S_{i+2}, \ldots, G_j, N_r)_{K_p} \} \quad (5)$$

When the source sensor node receives the RREP message which replied by the intermediate sensor node, it has to authenticate the path list. In this case, the path list has two parts: the signed path (which it has been signed by the gateway) and ordinary part, which the other nodes form it. The source sensor node can authenticate the signed part with the public key of the gateways. The serial number into the signed part helps to the source sensor node to detect replayed message from other rounds. For authenticating the ordinary part, the sensor node saves $M_{S_0 S_1 \ldots S_i}$. When the source sensor node wants to sent its data, it appends $M_{S_0 S_1 \ldots S_i}$ and ordinary part to the first data. When the gateway receives the first data, it verifies the received MAC value with shared keys between it and the sensor nodes which are in the received ordinary part. After that, the gateway informs the source sensor node with a message which it signed by the private key mesh nodes (K_p).

IV. Mobility of Wireless Mesh Gateways

As mentioned in previous section, the WMGs can move into the sensor network. The movement of the WMGs should be in radio range of the sensor nodes and their communication does not have to be interrupted. This movement is not continuous and it is periodically. In each *round*, the topology of the network is fixed. For distinguishing the *round*s, a serial number (N_r) is used. When each gateway decides to move, it broadcasts a Notification message throughout the network to inform the other nodes. This message is signed with the private key (K_p). The notification message includes: type of message (*not*), gateway id (G_i), the serial number of the next *round* (N_r'), and serial number of the current *round* (N_r).

$$Notification = \{\text{not}, G_i, (N_r', N_r)_{K_p}\} \quad (6)$$

The gateway should get to the new place in a specific time. This time should not to be very long because a part of the network will be in an unconnected state and there is no communication in this part to the APs.

Each sensor node received a Notification message at the first time, it waits for a specific time and after that it can be sure the gateway has gotten to its new place.

Round's time can be computed by the gateways in two methods. First, the gateway has all communicated bits. With this information, it can estimate the energy consumption of its near sensor nodes. When the computed consumption energy is less than a threshold, the gateway decides to change its place. As second method, when the energy consumption of the nodes, which are around the gateway, exceeds a threshold, they inform the gateway. The gateway will move if considerable amount of the nodes inform their energy consumption.

V. Conclusions

The wireless sensor networks are a kind of networks which have many applied usage. The energy consumption and secure routing are essential issues in these networks. The nodes which are around the sink consume their energy more than the other nodes. For distributing consumption of the energy among nodes, this paper has presented a combination of the wireless mesh networks and the wireless sensor networks. In this architecture, the mesh gateways move in the sensor networks periodically. By moving the gateways, the nodes which are around the gateways change and energy consumption will distribute. In addition, this paper has proposed a secure routing algorithm for this new architecture. This algorithm presents a method that the intermediate nodes are able to respond to a route request message (RREQ). The intermediate nodes can update their routing table when forward the reply messages (RREP). By applying this algorithm, the malicious nodes do not able to remove the nodes of the path list and show a short route.

References

[1] J. N. Al-Karaki and A. E. Kamal, "Routing techniques in wireless sensor networks: A survey," *IEEE Wireless Communications*, vol. 11, no. 6, pp. 6–28, 2004.

[2] Y.-J. Lu and T.-L. Sheu, "An efficient routing scheme with optimal power controlin wireless multi-hop sensor networks," *Computer Communication*, pp. 2737-2743, 2007.

[3] E. Çayırcı and C. Rong, *Security in Wireless Ad Hoc and Sensor Networks*, John Wiley & Sons Publications, 2009.

[4] C. Intanagonwiwat, R. Govindan, and D. Estrin, "Directed diffusion: A scalable and robust communication paradigm for sensor networks," in *Proc. ACM MOBICOM*, pp. 56–67, Aug. 2000.

[5] W. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "Energy-efficient communication protocols for wireless microsensor networks," in *Proc. Hawaiians Int'l Conf. Syst. Science*, pp. 3005–3014, Jan. 2000,

[6] K. Mirzaei, S. Khorsandi, and R. Enayatifar, "Energy-efficient routing security and control in wireless sensor networks," in *Proc. International Conference on Future Networks*, pp. 142–147, 2009.

[7] A. Boukerchea, R. N. Pazziaand, and R. B. Araujob, "Fault-tolerant wireless sensor network routing protocols for the supervision of context-aware physical environments," *J. Parallel Distrib. Comput*, vol. 66, pp. 586-599, 2006.

[8] F. Tang, M. Guo, M. Li, C.-L. Wang, and M. Dong, "Secure routing for wireless mesh sensor networks in pervasive environments," *International Journal of Intelligent Control and Systems*, vol. 12, no. 4, pp. 293-306, December 2007.

[9] X. Du, M. Guizani, X. Yang, and H.-H. Chen, "Two tier secure routing protocol for heterogeneous sensor networks," *IEEE Transactions on Wireless Communications*, vol. 6, no 9, pp. 3395-3401, 2007.

[10] M. Imani, M. Taheri, M. E. Rajabi, and M. Naderi, "Vulnerabilities in network layer at wireless mesh networks (WMNs)," *International Conference on Educational and Network Technology (ICENT 2010)*, vol. 1, pp. 478-492, June 2010.

Mohsen Imani received his BS degree in electrical engineering in 2004 from Shahrood University of Technology and his master degree in the same field from Iran University of Science and Technology (IUST) in 2011. He was a member of Secure System Lab at IUST from 2008 to 2011. His research interests are network security and communication networks. Currently, he is doing his PhD in computer science at the University of Texas at Arlington.