ALGORITHMS FOR SECURE ADDITION AND SEPARATION NODES IN WIRELESS SENSOR NETWORKS

LASHGARI, M.[1], MONTAZERI, M.A.[2], MEGHDADI, M.[3] , AFZALI, M.[1], ESFANDIARI, G.[2]*

[1] Department of Computer Engineering, Zanjan Branch, Islamic Azad University, Zanjan Iran
[2]Isfahan university of technology, [3] University of Zanjan
(phone: +98-9177065114; fax: +98-3113915199)

**e-mail:s_lsh2002@yahoo.co.uk*

***Abstract**. Wireless Sensor Networks (WSNs) are collections of large number of low-cost and low-power nodes with sensing, computation, and wireless communications capabilities. These nodes are often placed in a physically insecure environment and linked together by a wireless medium. As a result, these networks are vulnerable to different types of intentional or unintentional attacks. Some of attacks are originated from faulty or compromised nodes and some other becomes feasible when one or more sensor nodes are being added to or removed from the network. Therefore, utilizing efficient management schemes for adding or removing the sensor nodes to or from the network may result in counteracting many attacks. In this paper, we have proposed algorithms for secure addition and separation of nodes as well as secure message transmission in the cluster-based WSNs. It is mentioned that the presented algorithms are able to effectively counteract most routing attacks and provide the network security requirements.*

***Keywords:** Wireless Sensor Network, Addition, Separation, Security, Attacks.*

Introduction

Wireless sensor networks are new technologies which can gather and process data in sensitive environments. These networks are composed of one or several Base Stations(BS) and a large number of inexpensive and small sensor nodes. The sensor nodes, in contrast to base stations, are featured with limited energy, computation and transmission power. Base stations are required equipments which act as intermediate between the sensor network and the end user (Akyildiz, I.F., Su, W., Cayirci, E., 2002). In most WSNs, due to large scale of the network, limited transmission power of the nodes and existence of obstacles such as tall buildings or mounts, it is not possible for all nodes to directly communicate with the BS or other nodes. As a result, they communicate with the base station in a multi-hop manner (Holger, K., Willig, A., 2003). Utilizing efficient routing schemes are of crucial importance, because it greatly effects the factors such as energy consumption, transmission delay, amount of sent data and the network error tolerance (Holger, K., Andreas W., 2005).

Routing protocol consists of algorithms used to determine the best path to any given destination within the network. Many routing protocols choose the best path based on metrics such as the minimum number of hops, minimum energy consumption and the shortest distance.consequently, the lifetime of the entire network is increased (Kemal A., Mohamed Y., 2005). WSNs are exposed to damages caused by different unintentional or intentional attacks (Yanli Y., Keqiu L., Wanlei Z., Ping L., 2012). Some of attacks are originated from faulty or compromised nodes and some other becomes feasible when one or more sensor nodes are being added to or removed from the network. Therefore, utilizing efficient management schemes for adding or removing the sensor nodes to or from the network may result in counteracting many attacks (John, P., Walters, Z., 2006). WSNs ensure a wide range of applications, starting from security surveillance in *military and battlefields, monitoring previously unobserved environmental phenomena, smart homes and offices, improved healthcare, industrial diagnosis, and many more. Hence, securing these networks is of utmost importance. The existing security schemes in the field of ad hoc networks are not apllicable to wireless sensor networks due to afformentioned limitations of these networks. Moreover, most of the routing protocols of the wireless sensor networks have been developed without considering different aspects of security.(Harmandeep, S., Garima, M., 2011).*

In this paper, new algorithms are presented for secure addition and separation of nodes as well as secure message transmission in hierarchical cluster-based WSNs. Our proposed algorithms are characterized by features such as Low computational overhead, Considering alternative routes, low energy consumption and the scalability.

The rest of the paper is organised as follows: in section two, the hierarchical cluster-based routing protocols are introduced. The proposed algorithms for secure omission and addition of nodes and also transmission of messages in WSNs are discussed in the third section. In the fourth section, we evaluate our proposed algorithms and finally the last section is dedicated to the conclusion of this paper.

Hierarchical cluster-based routing protocols

As shown in Figure 1, a hierarchical approach breaks the network into clustered layers. Nodes are grouped into clusters with a Cluster Head (CH) that has the responsibility of routing from the cluster to the other cluster heads or base stations In networks with such structure, least attacks are applicable and if a node is conquered, its conquering effect is local. Beside, utilizing the concept of hierarchical structure, different levels of safety can be created in the whole network (Patel, S., Singh, A. K., 2012).

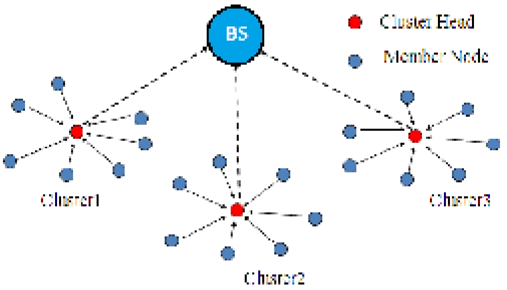

Figure 1. *An example of cluster-based sensor networks*

The proposed Algorithms for secure addition and separation of nodes in WSNs

In this section the proposed algorithms for securely adding and separating nodes in the single and multi-hop WSNs are described.

Key distribution

Each node in WSN shall be able to have message exchange by the BS, CH and some nodes inside the network. Therefore, it is required to determine common key between them. For each node, two types of keys are defined; main keys which are used for communication with BS and the CH, and auxiliary keys which are used for communication with the related nodes inside the network. when a node is entering the network, it's ID, the common keys planned for communicating with the BS and the CH *and the time interval within which the node can join the network are sent to the BS via a secure link. By receiving the abovementioned information and by taking the networks' pre-designed objectives into account, the base station creates a table for that node. For instance, table 1 is made for the typical node A. this table provides information about the nodes which are in connection with the node A.*

***Table 1.** table of a node code data*

ID=0125			*Time interval which the node can join the network=31 JAN, 8-16*				
Row	*Related nodes*	*Sender/ receiver*	*Min. Send Message per T.U.*	*Max. Send. Message per T.U.*	*Min. Rec. message per T.U.*	*Max. Rec. message per T.U.*	*Common secret key*
1	CH_i	*TR*	*0*	*2*	*0*	*3*	K_{A_CHi}
2	*B*	*T*	*1*	*5*	*0*	*0*	K_{A_B}
3	*C*	*R*	*0*	*0*	*0*	*0*	K_{A_C}
4	*D*	*TR*	*2*	*5*	*0*	*3*	K_{A_D}
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮

Notations

In order to simplify the algorithm description; some symbols are defined as below:

$$A \rightarrow B \;:\; A, B, \{Data\}_{K_{A\_B}} \tag{1}$$

It means that the Node A wants to send a message to the Node B. in this message, the sender and the receiver are specified. K_{A_B} *is common secret key between Node A and B. Also* $\{Data\}_{K_{A\_B}}$ *means that the data is encrypted by* K_{A_B} *.*

$$A \underset{\rightarrow}{B} C \;:\; A, C, \{\{Data\}_{K_{A\_B}}, B\}_{K_{A\_C}} \tag{2}$$

It means that node A wants to send a message to the node B where the node C acts as intermediary between them.

$$C \underset{\longrightarrow}{M\{A\}} B \;:\; C, B, \{A, \{Data\}_{K_{A\_B}}\}_{K_{C\_B}} \tag{3}$$

It means that node C wants to transfer the message of node A to the node B.

$$C \underset{\longrightarrow}{M\{A,B\}} D \;:\; C, D, \{A, \{Data\}_{K_{A\_B}}, B\}_{K_{C\_D}} \tag{4}$$

It means that node C wants to transfer a message which is originated from the node A and is destined for the node B, through node D.

The Algorithm for adding nodes in single-hop WSNs

Assuming that the network communications are taken place in a single-hop manner, figure 2 depicts the algorithm for addition of a typical node A to the cluster i in the network. Before entrance of the node A to the network, it's ID, main secret key and it's common secret key with the CH_i *and the time interval that the node is allowed to join the network are sent to the BS via a secure link. The base station creates a table as shown in table 1 for the node A. Before starting time interval which the node can join the network, the BS sends the data of table for related cluster heads. In order to join the network, node A, first sends its request to the* CH_i*.*

$$A \rightarrow CH_i \;:\; A, CH_i, \{JR\}_{K_{A\_CH_i}} \tag{5}$$

After sending the above request, if node A does not receive the CH_i response within a time unit, it will resend the request. If CH_i doesn't receive the message properly, or the code key is wrong, CH_i increments the appropriate counter which indicates the number of messages received from node A in a time unit. At the beginning of each time unit, this counter is reset.

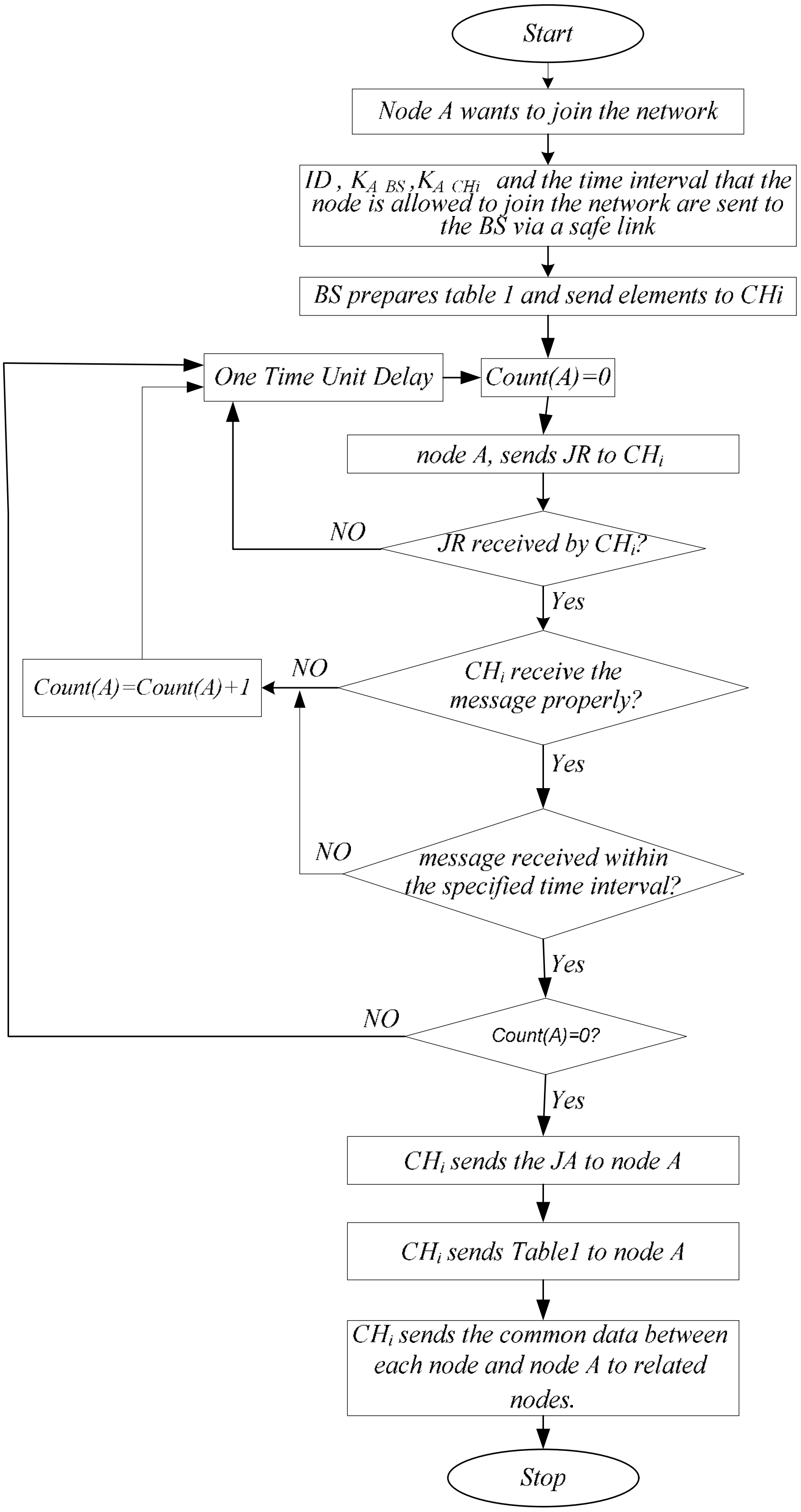
Start
Node A wants to join the network
ID , $K_{A\ BS}$,$K_{A\ CHi}$ and the time interval that the node is allowed to join the network are sent to the BS via a safe link
BS prepares table 1 and send elements to CHi
One Time Unit Delay
Count(A)=0
node A, sends JR to CH_i
NO
JR received by CH_i?
Yes
Count(A)=Count(A)+1
NO
CH_i receive the message properly?
Yes
NO
message received within the specified time interval?
Yes
NO
Count(A)=0?
Yes
CH_i sends the JA to node A
CH_i sends Table1 to node A
CH_i sends the common data between each node and node A to related nodes.
Stop

Figure 2. *Algorithm for addition of a typical node A to the cluster i*

When CH_i receives the message properly with the correct secret key, it investigates whether the message is received within the time interval specified in table 1 or not? If not, the counter related to the number of messages received from node A is incremented. If the message is received within the allowed time interval, CH_i investigates whether the number of the messages received from node A within the time interval is more than zero or not? If it is equal to zero, it is assumed as acceptance of request for joining node A to cluster i. At this time, the CH_i sends the response for the acceptance of addition (JA) for the node A. also, the CH_i sends the data of table 1 to the node A.

$$CH_i \rightarrow A: CH_i, A, \{JA\}_{K_{A\_CH_i}} \tag{6}$$

$$CH_i \rightarrow A: CH_i, A, \{Table1\}_{K_{A\_CH_i}} \tag{7}$$

Then CH_i sends a message to the nodes listed in it's table to inform the addition of node A to the network. . Also the common data between each node and the node A are extracted from the table and sent for related node. At this time, node A has joined the network and can exchange with CH_i and the nodes specified in table based on certain regulations.

The Algorithm for separating nodes in single-hop WSNs

In figure 3, the algorithm for separation of a node from cluster i in a single-hop WSN is displayed. In two cases a node may separate from the network. wether the node wants to get out of network on purpose and for making repair or change of parts or the node has got out of network extraordinarily and due to destruction of one of the main parts or conquer by enemy.

If the node wants to get out of the network on purpose, the time interval which this node is allowed to send the request of separation (RR) shall be sent to the base station via a secure link. Then, the base station informs the respective cluster head (CH_i). After the node A sends the request of separation to the CH_i, if the message is sent within the allowed time interval, CH_i sends a message backto the node A that it can leave the network. Also it sends messages to other nodes related to the node A that the node A has left the network and it gives orders for omission of all common keys between those nodes and node A.

If the node leaves the network due to reasons such as destruction of one of the main parts or conquers by enemy or it might not perform its duties within the framework defined, it is required for the CH_i to solve the problem and inform the base station and other nodes. In this state, CH_i is informed from emergence of interruption in the function of node A per following methods:

A) If node A sends the message for another node such as B in three consecutive time intervals lower than minimum defined in table 1, at this time, node B informs CH_i, then CH_i sends a message for node A directly and if it doesn't receive a response, it will inform other nodes related to the node A that node A has left the network and it gives order for omission of all keys related to that node. In figure 4, the steps for omission of node from cluster i in a single-hop network is displayed.

B) If node A does not respond to a message sent by another node such as B for three consecutive times, node B transfers this issue to CH_i, CH_i sends a message for node A directly and if it doesn't receive a response, it will inform other nodes related to node A that node A has left the network and it gives order for omission of all keys related to that node.

C) If node A sends messages for another node such as B more than maximum defined in a time unit, node B transfers this issue to CH_i, CH_i orders node B to stop its relation with node A and to omit all common key between that node and node A. at this time, there is no need for CH_i to inform other nodes. because node B might have sent wrong report for CH_i due to being conquered by enemy. In figure 6, the steps for omission of node from cluster i in a single-hop network resulting from message transfer over the maximum allowed messages.

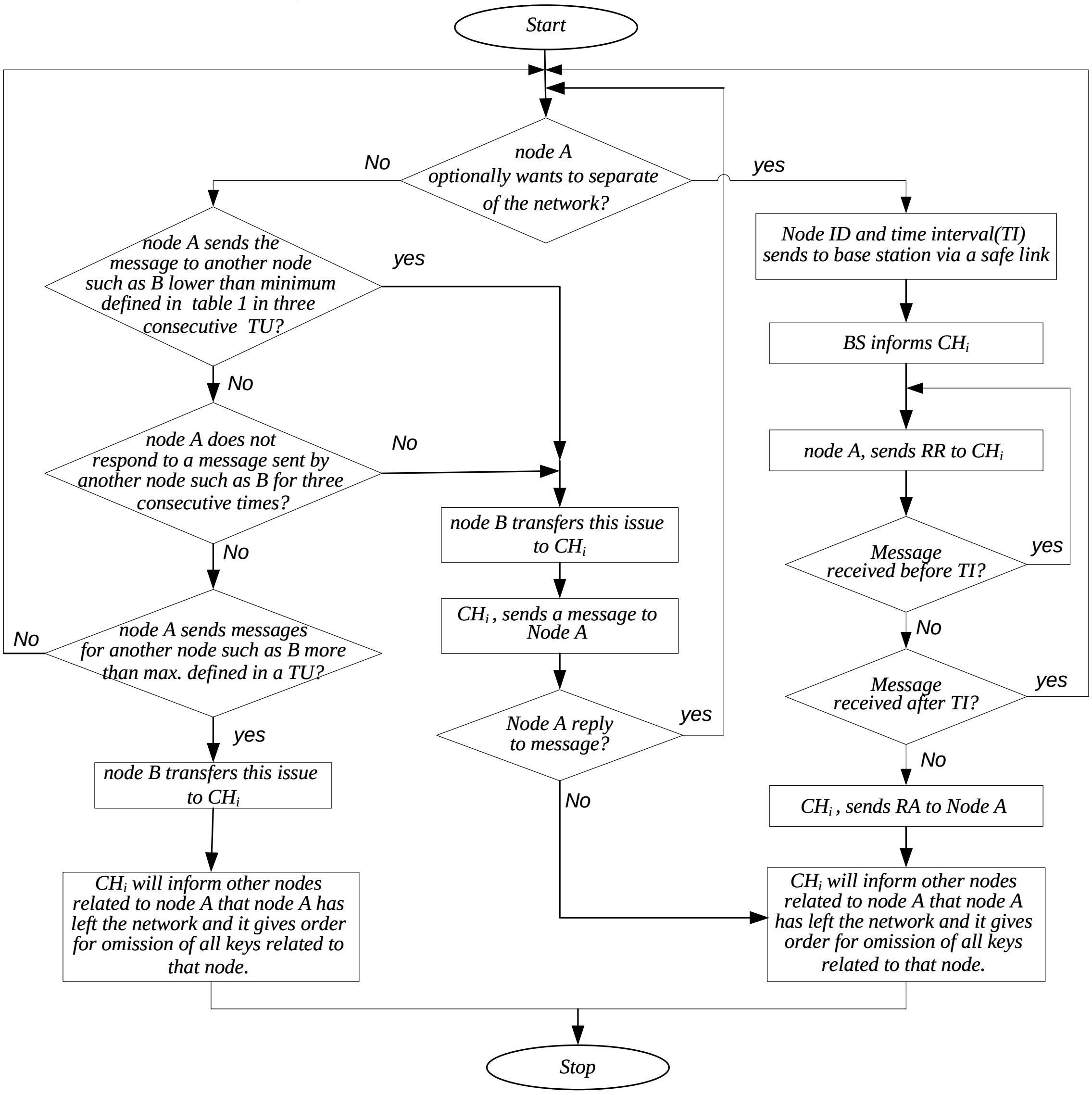
Start
node A optionally wants to separate of the network?
No
yes
node A sends the message to another node such as B lower than minimum defined in table 1 in three consecutive TU?
yes
No
node A does not respond to a message sent by another node such as B for three consecutive times?
No
No
node A sends messages for another node such as B more than max. defined in a TU?
No
yes
node B transfers this issue to CHi
CHi will inform other nodes related to node A that node A has left the network and it gives order for omission of all keys related to that node.
node B transfers this issue to CHi
CHi , sends a message to Node A
Node A reply to message?
yes
No
Node ID and time interval(TI) sends to base station via a safe link
BS informs CHi
node A, sends RR to CHi
Message received before TI?
yes
No
Message received after TI?
yes
No
CHi , sends RA to Node A
CHi will inform other nodes related to node A that node A has left the network and it gives order for omission of all keys related to that node.
Stop

Figure 3. *The steps for separation of a node from cluster i in a single-hop WSN*

Expansion of above algorithms in multi-hop network

In a single-hop network, it is required to specify the node's ID, node's main key, the common key with the cluster head and also the time interval which the node is allowed to join the network right at the entrance of node. In multi-hop networks, another key (K_{A_all}) is required for the node with which it can send the request for joining the network for adjacent nodes. Before the node enters the network, node's ID, three *aforementioned keys and the time interval within which the node is allowed to join the network are sent for the base station via a secure link. The base station will send the data of table 1 for the cluster head except the elements of first row and key K_{A_all}. At the beginning of time interval which node A is allowed to join the network, the cluster head informs other nodes inside ID network and K_{A_all} that this node can send the request for joining the network. When entering the network, node A sends its request for joining to the network as follows:*

$$A \rightarrow all\ :\ A, all\ , \{JR\}_{K_{A\_all}} \qquad (8)$$

Each of nodes which receive the massage of node A directly, via their path transfer the massage of node A to their cluster head. If the message is received within the accepted time interval, the cluster head by using one of routing protocols chooses the best path for transmission of message from node A to cluster head and other cooperating nodes.

The cluster head has also selected other substituting paths and saves them in the memory and in case that to any reason the main path is interrupted, it sends its messages and the new routing table for that node via substitute path in a higher priority. In addition, provides a table similar to Table 2 for that node. Table 2 is the completed form of table 1, with a new column called "Intermediate node" being added to that. In fact, node A by using this column, notices that through which nodes to send the sent messages to each of the corresponding (related) nodes. Then, through the selected direction, and using the secret key code, will send the acception message of being connected to the network, and also the table 2, to that node. The cluster head also sends the message of node A to those nodes specified in table 2, as well. It also extracts the common information between each node and node A from table 2, and sends them to the related nodes. At this moment, node A is connected to the network, and according to the rules specified in table 2, can continue its activities.

***Table 2.** table of code data of typical node A in Multi-hop WSN*

<table>
<tr><td colspan="3">ID=0125</td><td colspan="6">Time interval which the node can join the network=31 JAN, 8-16</td></tr>
<tr><td>Row</td><td>Related nodes</td><td>Send/ Rec.</td><td>Min. Send Message per T.U.</td><td>Max. Send. Message per T.U.</td><td>Min. Rec. message per T.U.</td><td>Max. Rec. message per T.U.</td><td>Common secret key</td><td>Intermediate Node.</td></tr>
<tr><td>1</td><td>CH_i</td><td>TR</td><td>0</td><td>2</td><td>0</td><td>3</td><td>K_{A_CHi}</td><td>C</td></tr>
<tr><td>2</td><td>B</td><td>T</td><td>1</td><td>5</td><td>0</td><td>0</td><td>K_{A_B}</td><td>D</td></tr>
<tr><td>3</td><td>C</td><td>R</td><td>0</td><td>0</td><td>0</td><td>0</td><td>K_{A_C}</td><td>C</td></tr>
<tr><td>4</td><td>D</td><td>TR</td><td>2</td><td>5</td><td>0</td><td>3</td><td>K_{A_D}</td><td>D</td></tr>
<tr><td>⋮</td><td>⋮</td><td>⋮</td><td>⋮</td><td>⋮</td><td>⋮</td><td>⋮</td><td>⋮</td><td>⋮</td></tr>
</table>

Separation of a node from a multi-hop network is similar to a single hop network, by this difference that in a single hop network if a node leaves the network, the routing is not interrupted, however in a multi-hop network, if a node like A which is leaving the network is in the path of message transmission between other nodes or nodes with cluster head, the cluster head informs other nodes via substitute path that node A has left the network and would send them the substitute path.

In order to save the originality and confidentiality of data, it is required for the sending, receiving and message transferring nodes to be specified and message transferring node shall not have the possibility to access message content. Assume that node A wants to transfer a message to node B via intermediate nodes C and D. in this case, data transmission would be as follow:

$$A \xrightarrow{B} C \ : \ A,C ,\{\{Data\}_{K_{A\_B}} ,B \}_{K_{A\_C}} \tag{9}$$

$$C \xrightarrow{M\{ A,B \}} D \ : \ C,D ,\{A,\{Data\}_{K_{A\_B}} ,B \}_{K_{C\_D}} \tag{10}$$

$$D \xrightarrow{M\{ A \}} B \ : \ D,B ,\{A,\{Data\}_{K_{A\_B}} \}_{K_{D\_B}} \tag{11}$$

Evaluation of the proposed algorithms

To evaluate the performance of the proposed algorithms, Some parameters, such as how to deal with the attacks, meet security requirements, additional memory and computational overhead needed to be considered.

Deal with attacks

A) Spoofed, Alerted, replayed routing information Attacks

In this attack, routing data between nodes are attacked. By performing spoofed, alerted, replayed routing information the invaders might be able to shorten or prolong source paths, create wrong error messages, divide the network and increase delay in network. In proposed algorithms, routing is conducted via cluster head and by addition or separation of a node from network, the cluster head sends the new routing information for related nodes, thus the invader node is not permitted to perform alert or fabrication of routing information of the network.

B) Selective Forwarding Attack

In a selective forwarding attack, unauthorized nodes might not send specific messages to next node and omit them. In proposed algorithms, by determination of appropriate amount for minimum number of sent messages for each node to other nodes or cluster head, this attack is controlled. By considering the importance of messages of each node, the cluster head determines this minimum amount. In case the adversary does not transfer some of the sent messages from node A to receiver, the receiver would realize that the number of sent data is less than the amount determined and would inform the cluster head.

C) Sink hole Attack

In this attack, a node with fabricated data and specifications misleads its adjacent nodes to give their information to it. At this time, the invader can alert, ruin or rob the content of received packs. Malicious node in fact announces wrong routing information. For instance, it announces that its distance to the base station is short. At this state, its neighbors are misled and they decide to choose it as their father. In this way, some of network nodes send their information for this node and this is where the invader can perform any malicious act. In proposed algorithms, data transmission path is selected by cluster head and by addition or separation of a node to network; the cluster head sends the new routing information for related nodes. Thus, the invader node is not allowed to introduce itself as father.

D) Hello Flood Attack

In this attack, an invader permanently sends a message containing request of communication to adjacent nodes. This message is usually sent by hello pack. In this state, by receiving hello pack the adjacent nodes are misled and they send a message for confirming the request, thinking that this relation would actually happen. This action is repeated till adjacent nodes lose their energy and turn off. In proposed algorithm, it is specified that by which nodes can each node communicate and maximum number of received messages are specified. Therefore, if a node seeks to send messages over the maximum allowed number, this issue is transferred to base station.

E) Sybil attack

In this attack, a malicious node pretends to be a number of nodes by fabrication of its identity. After the node injected different identities to the network, it takes action for deceiving legal nodes. In this way that it implies the legal nodes that its identities are communicative paths with other legal nodes. Besides interrupting routing protocol, this attack also interrupts voting protocols too and by using many identities, it can change the result of voting as it desires. In proposed algorithm, a node can be added to the network in a specific way and therefore a node cannot place itself as a number of other nodes.

F) Worm hole attack

In this attack, the invader connects two points of network via a relatively quick communicative bed which is called worm hole. This communicative bed can be wireless connection with a high range or even optical fiber. When the worm hole path was implemented, the invader conquers the packs sent by nodes from one side of the network and distributes them in the other side of the network via worm hole path. In this state, the nodes which are located in both sides of worm hole can ruin the packs or rob their contents and via this they can ruin the whole network's security. In proposed algorithms, routing is conducted via cluster head and by addition or separation of a node from network; the cluster head would send the new routing information for related nodes. Therefore, invader nodes are not allowed to create worm hole path.

Meet security requirements

In algorithms presented in this paper, Transmission of each message is done by coding and use of code keys, thus safety needs included of authentication, data authentication, access control, availability, privacy and secure channels are met. Each node can only communicate with nodes specified in table of that node, thus the security need of access control is met. By appropriate selection of minimum number of transferred messages for each node, security need of availability is met.

Computational overhead

The main computations which setting up of these algorithms add to an unsecure WSN are performed as for the key generation, key management, encryption and decryption of the messages; and to check the minimum and maximum conditions of the sent and the received messages. The key generation is performed in the BS which has a high computation power, and in this regard, no extra computation is imposed on the CH or the other nodes. In these algorithms, the decentralized management method is used which is one of the best key management methods. The BS is used as an acceptable center in the begining of the set up of the network, and also in order to add or separate *the nodes; and the CHs are used in the distribution and key management. In any sensor network which pays attention to the security, encryption and decryption of the messages is such a necessory act, and the operating system must be able to perform that. Checking the minimum and maximum conditions of the sent and the received messages doesn't have such a computation load and it is only few simple conditions.*

The additional memory needed

The additional memory needed in any node is used in order to save the existing data in the corresponding table of that node. Since in this table there are common keys with co-working nodes, there is no need to save the common keys with the other nodes of the system, and this way, the memory of each node is being used optimally.

Conclusion

In this paper, we proposed algorithms for secure addition and separation of nodes as well as secure message transmission in the hierarchical cluster-based WSNs.our algorithms are characterised by the features such as Low computational overhead, Considering alternative routes, energy saving and applicability for large-scale multi-hop sensor networks.

REFERENCES

[1] Akyildiz, I.F., Su, W., Cayirci, E. (2002): A survey on sensor networks, IEEE Communications Magazine, 40(8):102–114.

[2] Holger, K., Willig, A. (2003): A Short Survey of Wireless Sensor networks, TKN Technical Reports Series, Technical University Berlin, Berlin, pp. 1-19.

[3] Akyildiz, I.F., Su, W., Cayirci, E. (2002): Wireless sensor networks(A survey), Computer Networks Journal, Elsevier Science, Vol. 38, No. 4, pp 393–422.

[4] Holger, K., Andreas W. (2005): Protocols and Architectures for Wireless Sensor Networks, John Wiley & Sons, Ltd.

[5] Kemal A., Mohamed Y. (2005): A survey on routing protocols for wireless sensor networks, Science Direct, Ad Hoc Networks 3, 325–349.

[6] Yanli Y., Keqiu L., Wanlei Z., Ping L. (2012), Trust mechanisms in wireless sensor networks: Attack analysis and countermeasures, Journal of Network and Computer Applications, Volume 35, Issue 3, Pages 867–880.

[7] Karlof, C., Wagner, D. (2003): Secure routing in wireless sensor networks: Attacks and countermeasures, Ad-Hoc Networks Journal, vol. 1, pp. 293–315.

[8] John, P., Walters, Z. (2006): Wireless Sensor Network Security: A Survey Security, in Distributed, Grid, and Pervasive Computing Auerbach Pub., CRC Press.

[9] Harmandeep, S., Garima, M. (2011): Approaches to Wireless Sensor Network: Security Protocols, WCSIT Journal ISSN: 2221-0741 Vol. 1, No. 7,302-306.

[10] Parul, T., Surbhi, J. (2012): Comparative Study of Routing Protocols in Wireless Sensor Network, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 9.

[11] Patel, S., Singh, A. K. (2012): A Survey On Cluster Based Routing Protocol Organization For Wireless Sensor Network, Golden Research Thoughts, Volume 2, Issue. 4.