SRCDD: Secure Route Construction and Data Dissemination Protocol for Wireless Sensor Networks

Seyed Reza Taghizadeh

Department of Industrial Engineering, University of KNTU, Tehran, Iran

Dr. Shahriar Mohammadi

Department of Industrial Engineering, University of KNTU, Tehran, Iran

Abstract

As a consequence of widespread usage, wireless sensor networks has become a hot topic, and routing issues in wireless sensor networks have attracted many researchers. On of the most importing things in routing protocols is security issue. As a nature of wireless sensor networks, they are prone to many malicious actions. So the routing protocol should be secure enough to guarantee the data security. In this paper, we present a routing protocol, which is secure in both cases of route construction, and data dissemination. We have simulated this protocol using NS2.

Keywords: *Routing protocol, secure routing, data dissemination, wireless sensor network*

1. Introduction

in recent years great efforts have been made to make the networks secure, due to the expansion of network usage in all areas. Some security systems based on trust and reputation have been proposed, such as [1], [2], [3], [4].These security systems can improve the secure capability of application systems. Many protocols and algorithms, like DSR [5] and AODV [6], have been proposed for traditional wireless ad hoc networks. But they are not well suited for the unique features and application requirements of sensor networks because of many differences between sensor networks and ad hoc networks [7, 8]. These differences include the size of the network, communication patterns, and node capacity etc. In [9], a dynamic key distribution protocol -SDSK based on clustering is proposed, it considers both the residual energy of nodes and its location information to optimize cluster head election mechanism, and uses the dynamic key generated by hash functions to encrypt the data transmission. Compared to other clustering protocol, SDSK cuts down the energy consumption and extends the life cycle of WSN. In [10], a hash chain based random key pre-distribution scheme is proposed. Nodes only need to preload a few of secret keys and can establish pair-wise keys amongst its neighboring nodes with high probability through tuning some system parameters, such as the length of hash chain, the number of common auxiliary nodes, the number of hash chain.

In [11], a set of Security Protocols for Sensor Networks, SPINS, is presented. SPINS consists of SNEP and TESLA. SNEP provides the following important baseline security primitives: data confidentiality, two-party data authentication, and data freshness. TESLA is a new protocol which provides authenticated broadcast for severely resource-constrained environments. Its drawback is that energy costs so much in SNEP and TESLA maintenance phase. In [8], a new routing protocol called SEEM: Secure and Energy-Efficient Multi-path routing protocol is proposed. SEEM uses multi-path alternately as the path for communicating

between two nodes, thus it prolongs the lifetime of the network. Its advantages are mitigating the load of sensor nodes by transferring routing related tasks to the source, extending the lifetime of the whole network by using multi-path to transfer data, reducing the transmission delay through using the shortest and reliable path. ,

we focus on the cluster-based routing protocol's security issues by using the key management schemes. Most of them are designed for the multi-hop communications networks, and they are not well suitable for clusters-based routing protocols in WSNs. Among those specifically targeted of cluster-based sensor networks, Bohge et al. [12] proposed an authentication framework for a concrete 2-tier network organization, in which a middle tier of more powerful nodes between the SOURCE and the ordinary sensors were introduced for the purpose of carrying out authentication functions. In their solution, only the sensor nodes in the lowest tier do not perform public key operations. More recently, Oliveira et al. [13] proposed a solution that relies exclusively on symmetric key protocols and is suitable for networks with an arbitrary number of levels.

In this paper, we explain our proposed method, and also the security policies in chapter 2. Then we talk about the security issues of our proposed method, and analyze it to see whether it's secure enough or not, in chapter 3. simulation results are presented in chapter 4. And finally, chapter 5 concludes the paper, and defines some aims to be covered in future works.

2. Proposed method

2.1. Routing protocol Preliminaries:

The first thing that should be taken into the consideration is that in this model each node is equipped with a GPS device, so that it can send its location information to its neighbors. In this article we know $node_i$ as a neighbor of node*j* if there exist a connection between these two node after that the routing graph is made. We introduce some features for each node in the network. These features are kept by the source, and is used for graph construction, and routing information. The features are as follow:

Each node has a unique *ID*, and a *PL* field which shows the number of hops between the node and the source. Furthermore, there is a field for node type, which can have three different values: *CH* for cluster head, *CM* for cluster member, and *S* for source. The parent information is also kept in a separate filed. Beside these, source node computes a δ value, which will be explained later in this article.

2.2. Security policy preliminaries:

The propose model is secure in both cases of introducing the path to the nodes, and sending data. This security is achieved by some policies applied to the routing protocol on each phase. In order to apply these policies some specific parameters should be kept. These parameters are as follow:

Table 1 : Specific parameters used by security policies

Parameter	Description
$\mathbf{ID_i}$	The unique integer in network allocated to a sensor node.
$\mathbf{PL_i}$	Number of nodes between source and $node_i$
E(K,M)	Encrypts M with K
HMAC	Hashed Message Authentication Code
$\mathbf{P_i}$	Geographical position of node i
$\mathbf{Key_i}$	A pre-shared key which is stored by each node
$\mathbf{StKey_i}$	Key of $Subtree_i$
BSKey	Key of Source
$\mathbf{CKey_i}$	Key of $cluster_i$
KCM	Key Contained Message
$\mathbf{RPw_{I,t(n)}}$	Integer of Remaining Power of $node_i$ at time t
HMsg	Hashed message
$\mathbf{M_c}$	A message, containing some information

2.3. Secure Route Construction and Data Dissemination Protocol (SRCDD):

The routing protocol consists of five different phases, named as: Network structure recognition, selection criteria attribution, cluster haed selection, Route path construction, and data delivery. The security policy of each phase is also is defined at its end.

2.3.1. Network structure recognition:

In this phase, the source should achieve a comprehensive knowledge about the network, so that it can find the suitable path for routing data. To achieve this goal, each node in the networks sends two pieces of information to the source at first steps: its *ID*, and geographical position information which is kept in a field, named as *P*. this information is broadcasted in the form of a packet. After receiving the nodes packets, the source keeps them in a table, and goes to the next phase.

Security policies:

As we mentioned in above, in this phase the source tries to know the network, and this is done by the massages broadcasted by each node toward the source. To make this transaction secure, source tries to authenticate each node, so that it assures there is no intruder. This authentication is done by the key_i, which is a pre-shared key, stored by each node. So the *ID*, and *P* that are supposed to be sent by each node, are sent in the format described below:

$n_i \rightarrow S: ID_i , P_i , RPw_{i,t(1)} , HMAC (Key_i , P_i \ || \ ID \ || \ RPw_{I,t(1)})$

On reception, the *S* calculates the value of HMAC again, and compares it with the received one. If equal, S accepts the node as a legal one, and stores its RPw_i for next stages security policies. It also saves P_i to be used as a criterion for CH selection phase.

2.3.2. Selection criteria attribution:

In the proposed routing protocols, cluster heads are selected in accordance with two criteria: δ, and *PL*. In this phase, source first computes the Euclidean distance between each node and itself (d_i). After that it computes δ_I, which is computed as d_i divided by radio range of nodes (d_i/R). It should be considered that radio range is constant for all the nodes. In the next step, source makes the *PL* value of the nodes which are far less than its radio range to 0, and groups them with itself. After that, all the nodes in this group explore the nodes within their radio range, and set their *PL* to 1. This process is done again by the new group to set the *PL* value of remaining nodes, until all the nodes in the network are covered. Then *S* stores both δ and *PL* in a table (named as M_c), and broadcasts the table in the network. At reception, each node saves its δ and *PL* values.

Security policies:

As it is described in above, in this phase the main data flow is from the S toward the nodes. So security policies should focus on how to authenticate the SOURCE, and also make sure of received message integrity. Hence the policies are as follow:

S calculates: $KCM = E (Key_I , BSKey)$

Also calculates: $HMsg = HMAC (Key_i , P \ || \ M_c \ || \ KCM \ || \ RPW_i)$

Then it sends these two pieces of information as a unicast message, to each node:

$S \rightarrow n_i : P_i \ M_c , KCM , RPw_i , HMsg$

When a node receives this message, it first computes the HMAC value, just like what the SOURCE did before, to make sure of both authenticity of sender, and integrity of the message. After that it extracts the values of BSKey, and M_c for later use.

2.3.3. Cluster head selection:

At this phase, each node sets another node in its range, which has the least value of *PL* among the neighbors, as a candidate for cluster head, or in other words, as its preferred CH, and introduces it to the source. If two or more *PLs* happen to be equal, then selection is made in terms of δ value. The less value of δ, means the more probability of being chosen. Once all the nodes introduce their preferred CH, source starts choosing *CHs* according to a descendingly sorted list of preferred *CHs*, which is sorted according to number of request for each node to become a CH. At selection, each *CH* makes all nodes in its radio range as its cluster members (*CM*), and introduces them to the source, so that source excludes them from the sorted list, if any of them is contained in the list. To illustrate this process, we have shown a sample process in figure 1.

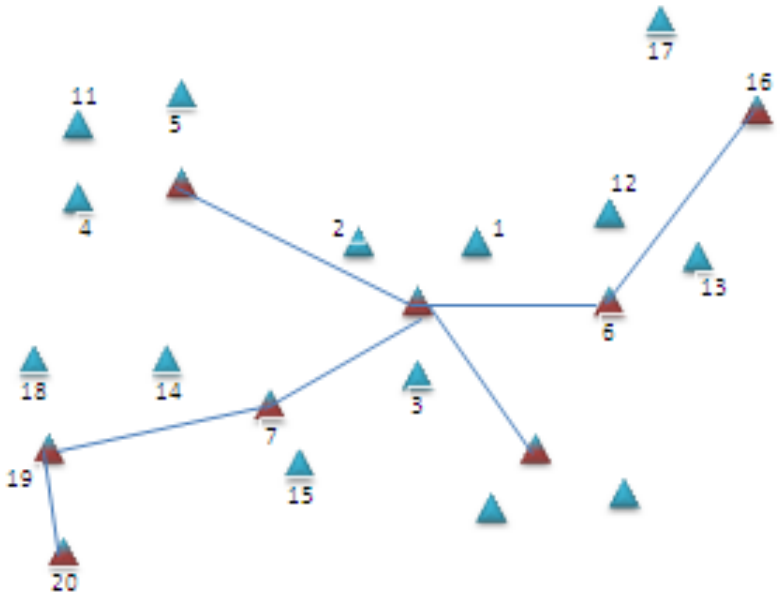

Figure 1: cluster head selection

Security policies:

The transaction of this phase is made secure in the following way:

$n_i \rightarrow S$: ID_i ,PCH , HMAC (Key_i , PCH || ID)

S calculates: M_c = E (Key_I ,CHList , BSKey || $CKey_i$)

Also calculates: HMsg = HMAC (Key_i , M_c)

$S \rightarrow n_i$: M_c , HMsg

Where PCH is Preferred Cluster Head, and $CKey_i$ is set to Null for those who are not selected as CH. Then the chosen node sends its member list to S, and forwards the received CKey toward CMs

$n_i \rightarrow S$: ID_i ,CMList , $RPw_{i,t(2)}$, HMAC (Key_i , CMList || ID)

$n_i \rightarrow CM_j$:E (Key_j , $CKey_i$) , HMAC (Key_i , E (Key_j , $CKey_i$))

2.3.4. Route graph construction:

Route graph is made in a bottom-up manner. It means, the route is made from the furthest nodes up to the source. The remoteness of nodes is defined as the value of their *PL*s. in this view, the farthest node start constructing the route graph as follow:

Firstly the node with maximum value of PL is chosen, and becomes a start point to construct a subtree. In our example, this node is n29. Then the algorithm chooses the nodes in a backward direction: n29, n33, n32 and finally n25. Now the path has arrived at a child tree root node. So the algorithm names the found subtree as Subtree(0), and starts again with the next maximum PL value node, to find the next subtree. This procedure is done until all nodes are covered. This process is shown in figure 2.

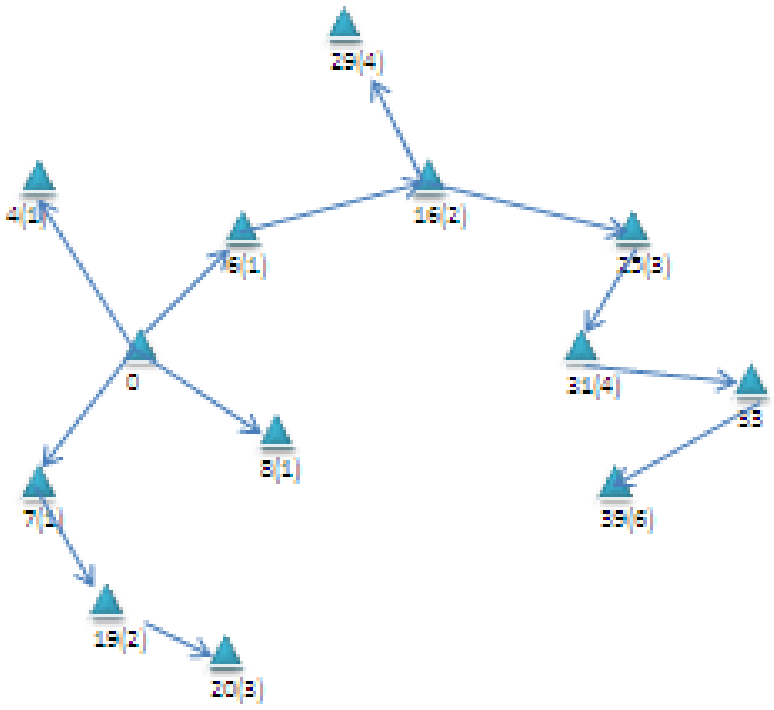

Figure 2: Route graph construction

Security policies:

The information of subtree structure is sent to all nodes, as follow:

$S \rightarrow * : E (Key_i , StKey_I || M_c) , HMAC (Key_i , E (Key_i , StKey_I || M_c))$

In which M_c contains information about subtree topology structure.

2.3.5. Data dissemination:

When the source wants to send any data, it chooses the related subtree, and sends the data toward it .when the message arrives at the subtree root node, it will be forwarded by the cluster heads, which are inside the mentioned subtree, in terms of *CHs' PL* value. As a *CH* detects itself as a destination, it broadcast the content of the message.

Security policies:

This phase is planned for data dissemination. So this is the most important and also most frequently used phase. A probable intruder puts most of his/her effort to abuse transmitted packets, since they carry nodes sensed some data. So consequently it should be secure enough. This phase, makes use of another parameter, cited as RP_w:

$S \rightarrow * : E (StKey_i , Data) , HMAC (StKey_i , E (StKey_i , Data))$

As the message reaches the destination subtree, all CHs in the subtree multicast the message:

$CH_i \rightarrow CMs : E(CKey_i , Data) , HMAC (E(CKey_i , Data))$

Then they reply to S in this way:

$CH_i \rightarrow S : ID_i , E (CKey_i , RPw_{i,t(n)}) , HMAC (E (CKey_i , RPw_{i,t(n)}))$

When S receives this message, it computes $RPw_{i,t(n)} / RPw_{i,t(n-1)}$. We name this portion as ω_n .

if $|\omega_n-\omega_{n-1}|$ > threshold, or $RPw_{i,t(n)} > RPw_{i,t(n-1)}$, then S recognize that either this node is malicious or is under attack. It should be mentioned that S saves three sequences of received RPWs for each node.

3. Security analysis

In this chapter we analyze our protocol to see whether it's secure or not

3.1. Data security:

Integrity and verifiability are two important factors in data security. All transmitted messages use keyed-Hash Message Authentication Code (*HMAC*) to guarantee the data integrity. Besides, using a secret key to compute the output, HMAC function makes it possible for the destination to validate the received message. On the other hand, since the data packet includes $RPw_{i,t(n)}$, it is is nor possible for an intruder to perform a reply attack. Above all, all of the messages disseminated from source, including CH information, graph topology, and data packets, are encrypted, using an encryption key.

3.2. Interception:

Since each node holds a Key_i , it is impossible for an intruder to find key by intercepting the transmitted messages. On the other hand, the attacker cannot extract the Key from HMAC since HMAC in a hashed value and hence irreversible. The only thing an intruder can obtain is HMAC value that is totally unusable.

3.3. Forgery of nodes and routing information:

In network structure recognition, and cluster head selection phases, the source sends some pieces of information to all nodes. They are not encrypted to free the destination of performing an unnecessary power consuming action of decryption, but it doesn't endanger the security, since an adversary who wants to modify the node-state information table cannot recalculate *HMAC* , due to lake of secret key. Hence in most of attacks intruders exploit these messages, this is a very effective procedure to combat network structure disclosure.

4. Simulation results

We evaluated the effects of probabilistic keying on secure routing using the Network Simulator (ns-2) version 2.27. Each simulation was run over two different field configurations: 200 and 500 nodes in a 500m x 500m test-bed. Nodes were given a maximum transmission range of 75m and used an 802.11 MAC layer. Initial node placements and their subsequent movements were generated by ns-2's included scenario generation utility. The keys stored in each of the nodes were generated a priori using the library function random(). As it's shown in figure * our protocol work better than shortest path tree (SPT) [8] as the number of destinations grows, but actually it has a better security guarantee. Figure* shows another comparison between these two protocols.

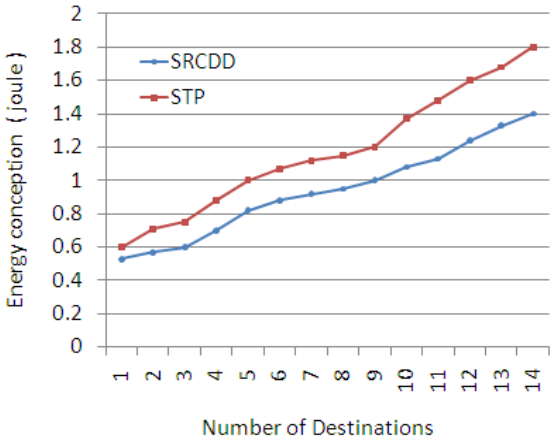

Figure 3: Effect of number of destination on energy conception

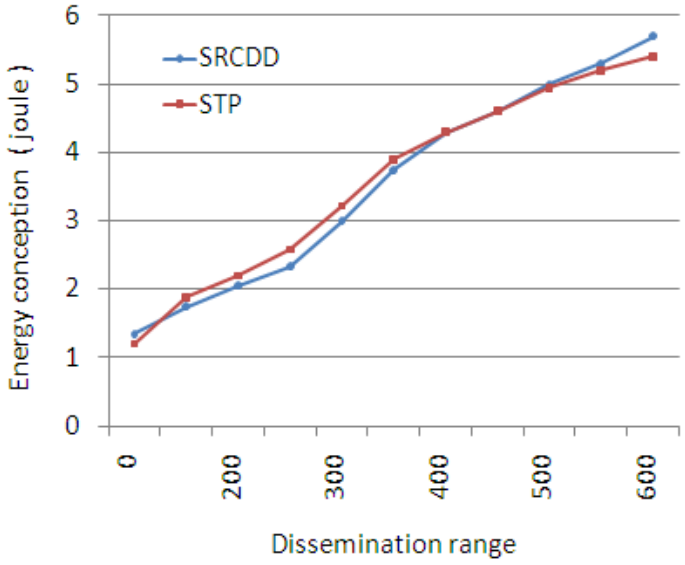

Figure 4: Effect of number of dissemination range on energy conception

5. Conclusions and future works

In this paper we presented a secure routing protocol for wireless sensor networks, which guarantees security in both route construction phase, and data dissemination phase. As it is shown in figures, it also consumes power efficiently, though this is not the main aim of the protocol. The protocol tries to minimize the transmitted packet in the network, and also to construct a path in an efficient way. We took advantage of encryption, and hashing to design this protocol. This protocol is based on hierarchical routing concepts. In the future works, we want to make this improve this protocol so that it supports mobility. We also want to expand the core routing procedure into a multipath routing procedure.

Acknowledgments

The authors would like to thank the Iran Telecommunication Research Center (ITRC) for serving as a sponsor and financial supporter of the current work.

References

[1] Xiao De-qin,FENG Jian-zhao, Zhou Quan, YANG Bo, Gauss reputation framework for sensor networks, Journal on Communication,Vol.(29),3,2008,pp.47-53.

[2] M.Blze,J.Feigenbaum,J.Ioannidis, A.D.Keromytis ,RFC 2704-The Keynote Trust Management System Version 2,Sep.1999.

[3] A.A. Pizada, C. McDonald, Establishing trust in pure ad-hoc networks, in: Proc. 27th Conf. Australasian Computer Sci. ACM int'l Conf. Proc. Series, Dunedin, New Zealand, 2004,pp.47-54.

[4] Heinzelman WR. Application-Specific protocol architectures for wireless networks [Ph.D. Thesis]. Boston: Massachusetts Institute of Technology, 2000.

[5] D. B. Johnson and D. A. Maltz, Dynamic Source Routing in Ad Hoc Wireless Networks, In Mobile Computing, Chapter 5, P153-181, Kluwer Academic Publishers, 1996.

[6] C. Perkins and E. Royer, Ad hoc On demand distance vector routing, Proc. 2nd IEEE Workshop Mobile Comp. Sys. & Apps., Feb 1999.

[7] A. Hac, Wireless Sensor Network Designs, 2003 John Wiley & Sons, Ltd, ISBN:0-470-86736-1.

[8] C. Hedrick, Routing Information Protocol, Internet Request For Comments RFC 1058, June 1988.

[9] Sanjay Sarma, Daniel W. Engels, "On the Future of RFID Tags and Protocols,"Auto-ID center white paper, June 1, 2003

[10] R.Peng, K.A.Hua, G.L Hamza-Lup, "A Web services environment for Internet-scale sensor computing," IEEE International Conference on Services Computing, 15-18 Sept. 2004 Page(s):101 – 108

[11] Aberer, Hauswirth, Salehi, "A middleware for fast and flexible sensor network deployment,"International Conference on Very Large Data Bases 2006, Korea."

[12] M. Bohge and W. Trappe. An authentication framework for hierarchical ad hoc sensor networks. In 2003 ACM workshop on Wireless security, pages 79-87, 2003.

[13] L. B. Oliveira, H. C. Wong, and A. A. F. Loureiro. Lha-sp: Secure protocols for hierarchical WSNs. In 9th IFIP/IEEE International Symposium on Integrated Network Management (IM'05), pages 31-44, 2005.

About The Authors

Seyed Reza Taghizadeh: He has received his bachelor degree in software engineering, and now is a master student of information technology in K.N.Toosi university of Tehran, Iran. His fields of interest are network security, routing algorithm of networks, and wireless sensor networks. He has taught different courses of network such as Network security, computer networks, and network lab. He is now working on his final thesis which is about wireless sensor networks security.

Dr. S. Mohammadi: He is a former senior lecturer at the University of Derby, UK. He also used to be a Network consultant in the UK for more than fifteen years. He is currently a lecturer in the Industrial Eng. Department of the University Of K.N.Toosi , of Iran. His main research interests and lectures are in the fields of Networking, Data Security, Network Security, e-commerce and e-commerce Security. He has published more than eighty papers in various journals and conferences as well as four books.