Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 5 (2011) 208–215

Procedia Computer Science

The 2nd International Conference on Ambient Systems, Networks and Technologies (ANT)

An Efficient Key Distribution Scheme to Secure Data-Centric Routing Protocols in Hierarchical Wireless Sensor Networks

Abderrahmen Guermazi[a], Mohamed Abid[b],a*

[a] *ISET Sfax, Road Mahdia B.P 88A ElBustan, Sfax 3099, Tunisia*
[b] *ENIS, Road Soukra B.P 1173, Sfax 3038, Tunisia*

Abstract

This paper deals with an efficient key distribution scheme which is useful to secure data-centric routing protocols in Wireless Sensor Networks. Similar to these routing protocols, the proposed scheme bootstraps secure key distribution with a centralized process which gives a multi-level hierarchical organization to WSNs. The originality of this work is to permit to use local key distribution process to establish Group Key and Pairwise Key. These two types of keys are useful to secure respectively data request diffusion and data forwarding through multi-hop routing paths. Moreover, when the WSN topology changes, the proposed scheme allows secure WSN reorganization. Security analysis explains that our proposed scheme can withstand several possible attacks against WSNs. A comparison to other solutions based on one KDC shows that the proposed scheme is significantly more efficient and scalable. This is well verified through simulations with TOSSIM under TinyOS using NesC language

Keywords: *Wireless sensor networks; key distribution scheme; secure routing; data-centric routing protocol*

1. Introduction

Many routing protocols are proposed to Wireless Sensor Networks (WSNs) [1]. However, in hostile environment, there are many attacks against WSNs and especially against routing protocols [2]. When routing protocol is compromised, there are fatal consequences on sensor network functioning like low availability, data diversion, energy dissipation and network disturbance. Security services for routing protocols are based on symmetric cryptographic algorithms which need key distribution mechanisms. In literature, some key establishment schemes are proposed for WSNs. However, most of them take in consideration neither the WSN organization nor the bootstrapping of the organization process (centralized, distributed…). In this paper, we are interested in proposing an efficient key distribution

* Corresponding author. Tel.: +216 25 488 172; fax: +216 74 431 386.
E-mail address: abderrahmen.guermazi@isetsf.rnu.tn .

1877–0509 © 2011 Published by Elsevier Ltd. Selection and/or peer-review under responsibility of Prof. Elhadi Shakshuki and Prof. Muhammad Younas.
doi:10.1016/j.procs.2011.07.028

scheme to secure data-centric routing protocols in homogenous WSNs. Thus, we suppose that sensor nodes have the same capabilities. In addition, they are deployed randomly in the investigated field.

The studied routing protocols are bootstrapped with a centralized process and provide a hierarchical organization to the WSN[3][4][5][6][7]. We recommend that the proposed key distribution scheme should be easily joined to the secure data-centric routing protocols. It must be able to share efficiently three types of keys: Global Key, Group Key and Pairwise Key to secure different communication patterns: one to all, one to many and one to one. Also, the proposed scheme should permit a secure WSN reorganization.

This paper is organized as follow: section 2 represents the background needed for our work, section 3 describes the key distribution scheme; section 4 contains a security analysis against the most known routing attacks; section 5 compares the scheme with other solutions; section 6 carries out simulations and results; section 7 concludes the paper.

2. Background

Routing in data-centric protocols is not based on address but rather on sensed data. Initially, the base station broadcasts a "Data Request" message. Sensor node which receives this message proceeds to broadcasted it again to all neighbors. After a period of time, "Data Request" messages arrive to the entire network. If a sensor node disposes data which satisfies the request, it sends a "Data Response" message via the best gradient (router). Data-centric routing protocols make it possible in-network processing (delete of redundant data, aggregation). It results from it a reduction of sending thereafter a reduction of possible collisions on the transmission channel. These aspects lead to energy saving and increasing network lifespan. For next interests, "Data Request" message can be sent by multi-cast to group nodes or by uni-cast to specific node. In the following, we give more details about data-centric routing protocols.

For « Directed Diffusion » [3], "Data Request" message represents an interest to data. Interest messages support attributes naming which specify a set of constraints to be met by sensed data which sink node expects, like class of data. It is possible to specify other parameters such as the interest expiration and the sending frequency. Thereafter, sensor nodes with data matching these constraints send data messages via all gradients. Whereas for « One Phase Pull » [4] –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 » [5] "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 » [6], routing metric is a function of consumed energy throughout the routing path. For « Gradient based routing » [7], sensor nodes keep the number of hops when the "Data Request" message is diffused through the network. Therefore, each node can discover the minimum number of hops to the sink, which is called height of the node. Thus, "Data Response" messages are forwarded via routing path having minimum gradients.

On the other hand, different key distribution schemes for WSNs are proposed in literature [8] [9]:

- 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 [10].
- Single network-wide key: a single key is preloaded into all nodes of the network. For example, Tinysec [11] 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 Pairwise Key sharing: for a network of n nodes, (n-1) Pairwise 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 [12]. This scheme isn't convenient to a centralized bootstrapping communication. Also it doesn't ensure that two nodes are always able to compute a Pairwise Key.
- Hierarchical key management: it supports various secure communication patterns: unicast, multicast and global broadcast. LEAP+ [13] is referred to as the basic scheme of hierarchical key management. LEAP+ initially establishes Pairwise 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 [14], 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 such scheme that is not scalable.

3. Description of the proposed scheme

Considering the particularity of routing in WSNs where “Data Response” messages are forwarded mainly to the base station, therefore "Data Request” messages received from nodes with higher height (further from the base station) will be rejected. In fact, for «Directed Diffusion» and «One Phase Pull» an interest message which is received from a data gradient is dropped. For « Energy-aware routing » protocol, routing path which contains subordinate nodes is obviously more expensive in terms of expended energy. For « Flooding and Gossiping » and « Gradient based routing », “Data Response” messages are forwarded towards base station. Consequently subordinate nodes shouldn’t belong to routing paths. Also in MTE [15], 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 metrics determine the best gradient. On the other hand, the hierarchical organization of the WSN offered by the routing protocols dedicates to establish Group Key for each group of nodes.

More precisely, the proposed key distribution scheme will have the following objectives:

- To perform a secure hierarchical organization of the WSN,
- To establish Group Key and Pairwise key,
- To cause low storage, computation and communication overhead
- To permit a secure reorganization of the WSN and to permit key refresh.

To reach the above objectives, the key distribution scheme must takes account of some characteristics:

- The studied routing protocols use a centralized process (initiated by the base station) to organize the WSN, then the key distribution process will proceed, in the same way, to give a secure organization.
- The first broadcast will be protected with a preloaded Global Key.
- The process to establish Group Key and PairwiseKey should be performed locally,

The key distribution scheme will need two phases to perform all these functionalities. Table 1 displays the notations used in this description.

Table 1. Notations table

Notation	Description
BS	Base Station
N	Sensor Node
GH	Group Head
*	Broadcast address
A ‖ B	Data A concatenated with data B
$MAC_K(A)$	MAC calculated and encrypted with a Key K
$Enc_{Key}(A)$	Encrypt data A with a Key K

3.1 Phase1: Secure organization of the WSN and Group Key distribution

Each node is preloaded with a Global Key. As the WSN is deployed, the base station proceeds by a secure broadcast of a “Path Discovery” message to trace routing paths. Eventually, this message will be used to distribute Group Key. To determine easily node level, a height field is added to the message. The height value received in the first message determines the node level.

$$BS \rightarrow * : \ * \| BS \| Nonce \| height \| Enc_{GlobalKey}(GroupKey) \| MAC_{GlobalKey}$$

Each node N receiving a secure "Path Discovery", it rebroadcasts this message after having been treated as it is shown in the flowchart (a) of Fig. 1. When the "Path Discovery" diffusion is achieved, the WSN is organized securely in hierarchical groups. More precisely, intermediate nodes are Group Head; each node N belongs to one or more groups with which it shares a Group Key. Finally, each sensor node deletes the preloaded Global Key from its memory.

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 [16] 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. Reminding that the key distribution scheme is proposed for homogeneous WSNs, we will keep 10 seconds as the necessary minimum time to reveal information from ordinary sensor node.

3.2. Phase 2: Pairwise Key distribution

At the end of "Path Discovery" diffusion, a node N sends a secure message "Join Group Request" to their Group Heads. Eventually, this message will be useful to share with each of them a Pairwise Key.

$$N \rightarrow GH: \quad GH \,||\, N \,||\, Nonce \,||\, Enc_{GroupKey}(PairwiseKey) \,||\, MAC_{GroupKey}$$

Thus, for each entry in the "Group Head cash" a node N proceeds as it is shown in first part of the flowchart (b) of Fig.1. When a "Join Group Request" message is received by a Group Head, it proceeds like it is shown in the second part of the flowchart (b) of Fig.1. The "Join Group Response" message is sent to a member group node N to confirm secure link:

$$GH \rightarrow N: \quad N \,||\, GH \,||\, Nonce \,||\, MAC_{PairwiseKey}$$

When phase 2 is achieved, a node N shares a Pairwise key with each Group Head (candidate router). After that, routing protocol determines the best gradient (router) towards base station.

3.3. Secure deployment of routing protocols

Once the two above phases are completed, the WSN is organized with a secure process which provides to each node secure link with candidate routers. Thus, for any studied routing protocol, the base station can initiate creation of secure routing path by diffusion of "Data Request" message which is protected with Group Key. Also, the intermediate nodes proceed with the same way, until leaf nodes of the network are reached. In consequence, each node having significant data, it will be able to send secure "Data Response", protected with Pairwise Key, via the best gradient.

It is obviously that a MAC field must be added to routing protocols messages to permit to check integrity and authenticity of the message origin. A flag can be added to indicate if the payload is encrypted.

3.4. Secure WSN Reorganization

When base station expresses a new need for data, the first phase of the routing protocol will consist in a secure diffusion of "Data Request" message. This allows a secure reorganization of the WSN, hence a secure retracing of multi-hop routing paths.

3.5. Key refresh

To maintain security in WSNs, shared keys should be efficiently refreshed with local process. Therefore, a Group Head can easily redistribute a Group Key with multicast message. Also, a group

member node can refresh Pairwise Key with the Group Head. Key refresh messages can be protected with shared keys. Further more, when a sensor node is compromised or it leaves the WSN, a non compromised node deletes the shared keys with it. Thus, a concerned Group Head initiates a local Group Key redistribution with each member protected by the Pairwise Key.

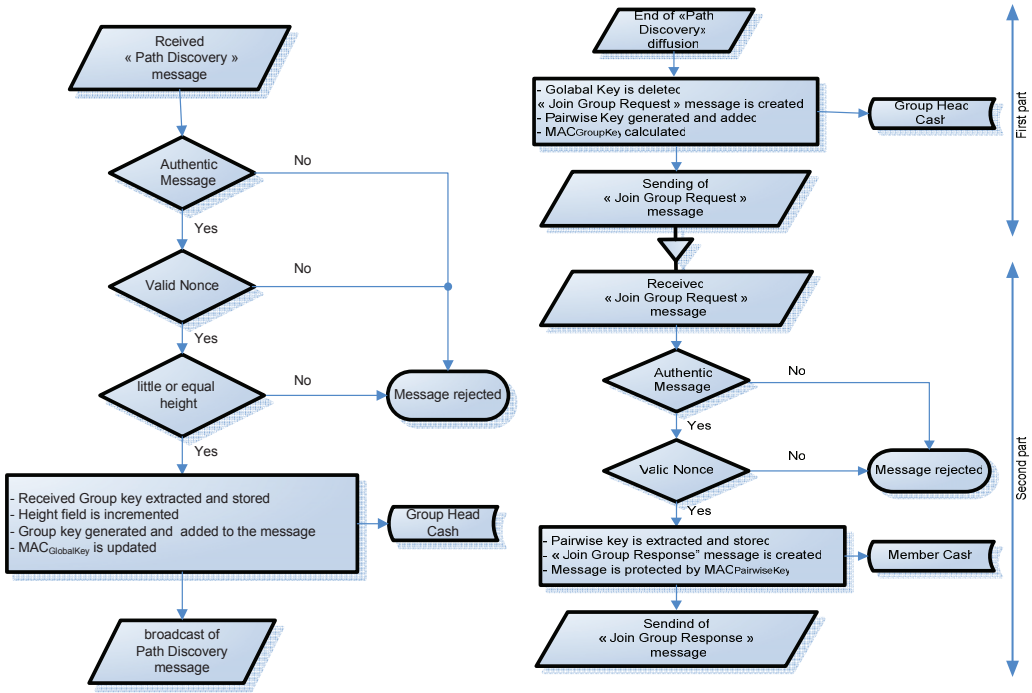

Fig. 1. (a) Flowchart of Group Key distribution process; (b) Flowchart of pairewise key distribution process

4. Security analysis

In this section, we are analyzing the immunity of the key distribution scheme against the most known attacks in WSNs.

- Data flow blocking: the key distribution scheme initiates communication by diffusion of “Path Discovery” message. This makes it difficult for an adversary to prevent the arrival of messages to sensor nodes.
- Physical attacks: In hostile environment, some sensor nodes can be captured and tampered. Obviously, the most sensitive information is shared keys. The impact of such attack affects only secure links with immediate neighbors and not the whole network.
- Replay attack: if an attacker tries to replay old messages, this does not hold because every node stores the last nonce.
- Black hole: if an attacker with high communication capabilities rebroadcasts a message, it cannot create a black hole in the WSN because it can't be authenticated by sensor nodes.
- Sybil attack : even if an attackers takes multiple identities, this does not hold because it can’t be authenticated
- Flooding attack: this attack does not hold because non authenticated message are rejected.
- Brute force attack: the secure key distribution scheme permits to refresh Group Key and Pairwise Key which limit the effect of this attack.

5. Comparison with other existing protocols

In literatures, other key pre-distribution schemes have been proposed for securing WSNs having similar organization. SNEP [14] 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 Pairwise Key, it is essential that they communicate with the base station which establishes a Pairwise Key for them. If the WSN uses multi-hop routing paths, SNEP will cause a high communication overhead. To reduce such required channel capacities a solution, in [17] consisting in incorporating SNEP in the routing protocol. As a result, messages size was increased. This is not effective because Pairwise Key refresh is not required in each data dissemination.

To authenticate the broadcast of "Path Discovery" message, neither asymmetric cryptography nor µTesla[8] is convenient. Indeed, asymmetric cryptography requires high computing. In addition, µTesla relies on the delayed disclosure key and one-way function key chains. It requires that base station and sensor nodes to be loosely time synchronized. Besides, the one-way key chain does not fit into the memory of a sensor node. As a result, µTesla only permit authenticated broadcast of the base station. However our key distribution scheme needs to authenticate also intermediate nodes (Group Heads) in order to share securely Group Key. The use of a preloaded Global key for limited period of time allows to cure these drawbacks. In fact, initial broadcast of "Path Discovery' message is authenticated and KDC functionalities are delegated to authenticated Group Head. All this prepares such solution to secure efficiently data-centric routing protocols mentioned above.

Our earlier work SecOPP [18], proposes a secure version of «One Phase Pull» protocol where the key distribution scheme is incorporated in the routing protocol. As a result, routing messages length increases for next subscription to data. Furthermore, concerning the routing protocols providing only one gradient, when a secure link between a source node and its gradient are lost, the source node will be unable to join the network during the next secure reorganization. As a consequence, source nodes will be isolated from the network as well as nodes which are connected to them. To overcome such a problem, our current key distribution protocol permits each node to share keys with several routers having little or equal height.

6. Simulations and results

To check functionalities of the proposed key distribution scheme, simulations are made with TOSSIM under TinyOS using NesC language [19] [20]. Sensor nodes are deployed in a random greed. Base station is located in the left higher corner. The signal range is about 10 feet. A lossy radio model is used with TOSSIM. Initially, we tested routing protocols to be protected with different network size. In order to make sure that sensed data arrives at the base station, we tested a light weight data centric routing protocol such as «One Phase Pull» diffusion. 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. Picture (a) of Fig. 2 shows the obtained topology when «One Phase Pull» is deployed to a WSN having 80 sensor nodes. Hence, we will be contented to secure these routing protocols for networks having less than 100 nodes.

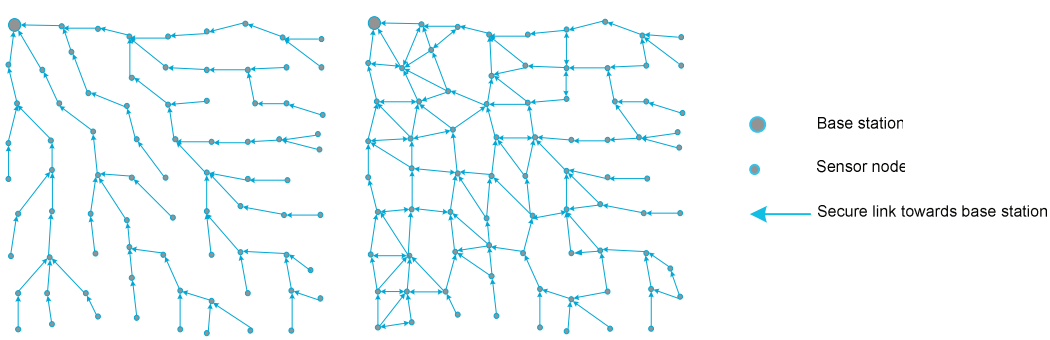

Fig. 2. (a) WSN topology obtained with OPP; (b) Secure WSN topology obtained with the key distribution scheme

Simulation results show that Group key and Pairwise key are well shared in the WSN. The picture (b) of Fig. 2 shows the obtained topology when the proposed key distribution scheme is performed. Indeed, the WSN is organized in hierarchical groups. Furthermore, it makes possible the nodes to have more than one secure link towards base station. Such topology provides a secure WSN reorganization.

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. Picture (a) of Fig. 3 shows the required time for different network size.

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 paragraph 5, the earlier works [14] [17] based on the use of one KDC are simulated with the same platform. The picture (b) of Fig. 3 presents 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.

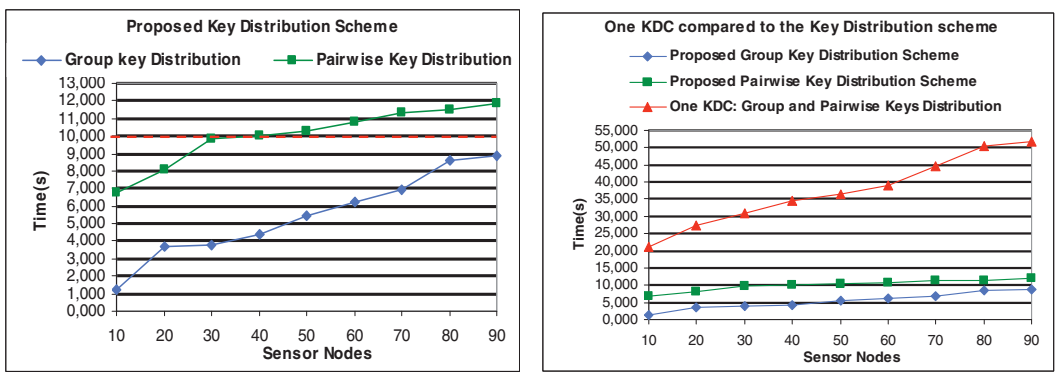

Fig. 3. (a) Proposed key distribution scheme: Time to distribute Group and Pairwise keys; (b) One KDC compared to the proposed scheme

To be sure that our key distribution scheme can be easily joined to data-centric protocols, it is simulated with the «One Phase Pull» for different network size. After key distribution, a secure interest message is diffused with such parameters: Attribute/value: temperature>40°C, Interest expiration is 200 Seconds, Sending frequency is 1. Simulation results show that sensed data reaches securely base station. In addition, execution time of this secure version is compared to the earlier work SecOPP [18]. Curves in the picture (a) of Fig. 4 show clearly that the proposed secure version of «One Phase Pull» diffusion routing protocol is more efficient than SecOPP.

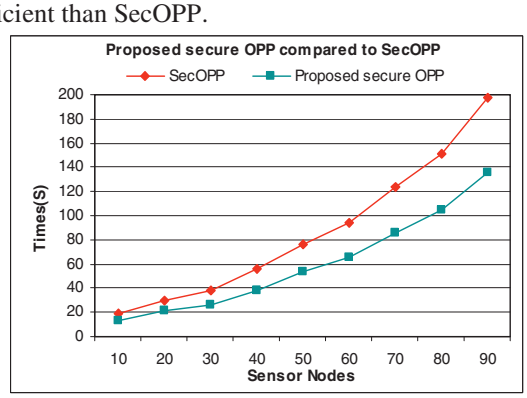

Fig. 4. (a) Comparison between SecOPP and the proposed secure OPP joined to the key distribution scheme

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 reorganisation. 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

[1] Kemal Akkaya, Mohamed Younis, A Survey on Routing Protocols for WSNs, *Elseiver Ad Hoc Networks* 3 (2005) 325–349

[2] C. Karlof and D. Wagner. Secure routing in wireless sensor networks: Attacks and countermeasures, *Elsevier's Ad-Hoc Networks Journal*, Special Issue on Sensor Network Applications and Protocols, 1(2–3):293–315, 2003.

[3] Chalermek Intanagonwiwat, Ramesh Govindan, Deborah Estrin , John Heidemann, Fabio, Silva, Directed diffusion for wireless sensor networking, *IEEE/ACM Transactions on Networking*, Volume 11 Issue 1, February 2003.

[4] Manamohan Mysore, Moshe Golan, Eric Osterweil, Deborah Estrin, Mohammad Rahimi, TinyDiffusion in the Extensible Sensing System at the James Reserve, http://www.cens.ucla.edu/~mmysore/ Design/OPP/, 2003.

[5] S. Hedetniemi, A. Liestman, A survey of gossiping and broadcasting in communication networks, *Networks*, Vol. 18, No. 4

[6] R. Shah & J. Rabaey, Energy Aware Routing for Low Energy Ad Hoc Sensor Networks, in *the Proceedings of the IEEE Wireless Communications and Networking Conference (WCNC)*, Orlando, FL, March 2002.

[7] C. Schurgers and M.B. Srivastava, Energy efficient routing in wireless sensor networks, *in the MILCOM Proceedings on Communications for Network-Centric Operations*: Creating the Information Force, McLean, VA, 2001.

[8] Marcos A. Simplício Jr. , Paulo S.L.M. Barreto, Cintia B. Margi, Tereza C.M.B. Carvalho, A survey on key management mechanisms for distributed Wireless Sensor Networks, *Computer Networks 54* (2010) 2591–2612.2.

[9] Junqi Zhang, Vijay Varadharajan ,Wireless sensor network key management survey and taxonomy, Science Direct, Journal of Network and Computer Applications. *Elsevier* 2009.

[10] An Liu and Peng Ning, TinyECC: A Configurable Library forElliptic Curve Cryptography in Wireless Sensor Networks, *in proceedings of 7th international conference on Information processing in sensor networks*, 2008.

[11] C. Karlof, N. Sastry, D. Wagner, TinySec: A Link Layer Security Architecture for Wireless Sensor Networks, *Proceedings of the 2nd International Conference on Embedded Networked Sensor Systems*, Baltimore, MD, USA, 03 – 05 November 2004, New York, NY, USA: ACM Press, 162 – 175. 2004.

[12] L. Eschenauer, V. Gligor, A key-management scheme for distributed sensor networks, *in: Proceedings of the Ninth ACM Conference on Computer and Communications Security (CCS'02)*, ACM, New York, NY, USA, 2002, pp. 41–47.

[13] Sencun Zhu, Sanjeev Setia and Sushil Jajodia, LEAP+: Efficient Security Mechanisms for Large-Scale Distributed Sensor Networks, *ACM Transactions on Sensor Networks*, November 2006.

[14] A. Perrig, R. Szewczyk, J. D. Tygar, V. Wen, and D. E. Culler, SPINS: security protocols for sensor networks, *Wireless Networks*, vol. 8, no. 5, pp. 521–534, 2002.

[15] Timothy Shepard. Decentralized Channel Management in Scalable Multihop Spread Spectrum Packet Radio Networks Report MIT/LCS/TR-670, Massachusetts Institute of Technology Laboratory for Computer Science, July 1995. Ph. D. Thesis.

[16] ANDERSON,R. AND KUHN, M. 1996. Tamper resistance—a cautionary note. *In Proceedings of the 2nd USENIX Workshop on Electronic Commerce'96*. 1–11

[17] Jibi Abraham, K S Ramanatha, An Efficient Protocol for Authentication and Initial Shared Key Establishment in Clustered Wireless Sensor Networks, *Proceeding of 3IFIP/IEEE International Conference on Wireless and Optical Communications Networks*, 2006, India

[18] Abderrahmen Guermazi, Mohmed Abid, SecOPP-a low-cost energy secure multi-hop routingprotocol for wireless sensor networks, Communication in Wireless Environments and Ubiquitous Systems: New Challenges (ICWUS), 2010 IEEE

[19] TinyOS: http://www.tinyos.net/, 2010.

[20] NesC: A Programming Language for Deeply Networked Systems. http://nescc.sourceforge.net/, 2010.