Investigating of an end to end security for wireless sensor networks

Ahmad Sharifi[1], Mohsen Khosravi[2], Hasan Sharifi[3], Jallaledin Sharifi[4]

[1.] School of Information Technology, Jawaharlal Nehru Technological University, Hyderabad, India
[2.] Faculty of Information and Communication Technology, International Islamic university Malaysia (IIUM)
[3.] Faculty of Management, Islamic Azad University of Shahrood, Iran
[4.] IT Section, Sharif Network Designers Company, Shahrood, Iran
ahmadsharifi.it@gmail.com

Abstract: Nowadays, providing security for Wireless Sensor Networks (WSNs) is an important subject. So, it is necessary to establish safety for sensors and sink, hence end to end services are emphasized. In this analysis, an end to end secure transmission procedure in arbitrary utilization of WSN was considered. The purpose of this study was improving flexibility of specific links by a methodology entitled differentiated key pre-distribution, including circulation of miscellaneous numbers of keys for different sensors. A higher resilience link was acquired by dissemination extra keys to some nodes.

[Ahmad Sharifi, Mohsen Khosravi, Hasan Sharifi, Jallaledin Sharifi. **Investigating of an end to end security for wireless sensor networks.** *N Y Sci J* 2016;9(2):12-18]. ISSN 1554-0200 (print); ISSN 2375-723X (online). http://www.sciencepub.net/newyork. 3. doi:10.7537/marsnys09021603.

Keywords: End to end security, Wireless Sensor Network (WSN), Distribution, Security, Sensor

1. Introduction

Today, Wireless Sensor Networks (WSNs) are visualized in warlike, crisis and observation implementations, where sensor nodes require forwarding perceived data to the sink. In numerous implementations subordinate to adverse circumstances, comprehensible deployment of sensor nodes is not affordable; consequently, they are anticipated to scatter haphazardly. A significant demand in network administration of various mission-critical petitions was adopted to secure end to end sensor network data, in order to restrain eavesdropping exploit. While, abundant activities have been accomplished on hop by hop invulnerable links. On the other hands, the content of the end to end secure communications was neglected. Communications through routing with activating were recommended to achieve end to end security. Balancing of the amount total of keys per node in plot and uniform key pre-distribution guarantees owning proper analysis.

Literature Review:

The elementary design for pre-distribution of arbitrary keys suggested, while the possibility of participation for one pairwise by various communications was a disadvantage [1]. Another q-composite plans presented [9]. It was protected by guarded route, including distinct keys constructing a trade-off between connectivity and invulnerability. Furthermore, in this accidental pairwise-key plan, a singular pairwise key was allocated to an arbitrary group and node. Although, intensive security was achieved, but it owns an upper bound on network proportion. It suggested the pairwise key pre-distribution idea derived on both the basic plot and Blom's plot, while receiving the threshold possessions. On the contrary, this study plan employs Blom's plan more effortlessly [4, 29-30]. Progression of key establishment accomplishment was purposed by deployment knowledge. There is threshold possession for the bivariate polynomials' usage. Connectivity and security of our design surpass former deployment knowledge. As it was mentioned before, the scheme in this study utilizes the deployment knowledge in a smoother way. Besides, Zhu demonstrated LEAP by establishing a slighter prototype concluding existence a momentary time interval whereas nodes which can substantiate pairwise keys that was firmly closed. Nevertheless, this time interval is frequently very tough to prognosticate precisely. Negotiating links in overvaluation circumstance was conceivable. Probabilistic Key Sharing considered the majority of the purposed symmetric key cryptography protocols for settling a pairwise shared keys between two nodes employing an on-line key server. Mitchell and Piper recommended a compound constructed on probabilistic key sharing that does not depend on such an online server. However, the storage complication compelled on each participator in their schedule looks to be unaffordable in the surroundings of ad hoc networks. The probabilistic key scheme in our protocol is corresponding to schemes that have been utilized by other investigators. Eschenauer and Gligor announced a key management scheme based on probabilistic key sharing for distributed sensor networks (DSN) with central key servers (e.g., Base Stations). Chan enlarged expanded this scheme by

proposing three recent mechanisms for key establishment in sensor networks. These networks are based on the structure of probabilistic key pre-deployment, including a mechanism for pairwise shared key establishment called multipath key support [5-10]. Some various point of this work was in comparison with preceding ones. First, in this system a node can derive the set of keys participating with any other node, maybe including vacant set, just depended on the last-mentioned individuality [11-14]. In the opposite, the approaches demand swapping of key identities among its neighbors. Consequently, our approach deals calculation for circulation that is a profitable factor in ad hoc networks. Second, Eschenauer and Gligor advised exploitation of the pre-deployed keys to encrypt all communications among nodes. A logical and pre-deployed keys' secure route organizes a session key between two nodes. With recognition pre-deployed key to several nodes, established session key does not acknowledge to the two involving nodes exclusively. In contrast, using the pre-deployed keys for setting up a shared pairwise key was designed which is known to two nodes exclusively with overwhelming possibility [15-19]. The idea of secret sharing is common in our both scheme and multipath key reinforcement, whereas the following dissimilar aspects are obvious. First, their design utilizes numerous actual disjoint paths between two nodes in planting a pairwise key, whereas our design can use an exclusive physical path as long as the shares are communicated over multiple logically disjoint paths. Second, it has been demonstrated a detailed security and fulfillment analysis of combining probabilistic key sharing and secret sharing, and also present an algorithm for deciding the number of confidential shares using for establishing a pairwise key based on the desired level of security. There has been a great amount of research on the threshold secret sharing Shamir and its applications. In one direction, Gong proposed an approach while threshold secret sharing was used to increment the availability of authentication services. Our process bears the correspondence that we also exploit secret sharing techniques to substantiate pairwise keys. Unlike Gong's design, our plot does not use any particular on-line key server. [20-24] In further relevant direction, investigators have highly explored the interplay of network connectivity and security with reliable communication.

Proposed Methodology: An honest party serves each cooperator a secret key and a public identifier, which facilitates any two contributors to produce a shared key for communicating independently. Every participator can create a shared key with any other participant, enabling secure communication to perform between any two members of the group [7-8]. Nevertheless, if an attacker can compromise the keys of at least k users, that can break the plan and reconstruct every shared key. [27-30] Blom's design is a format of threshold secret sharing. The key exchange protocol implicates a trusted party (Trent) and a group of n users. Fig.1, shows a user case diagram. Fig.2 accompanying fig.3 show key procedures. [31-38] Let Alice and Bob be two users of the group.

Protocol setup: Trent prefers an arbitrary and secret symmetric matrix Dk, k over the finite field GF (p), where p is a prime number [5]. While adding new user to the k sharing group, D is required for calculation.

For example, let $p = 17$, and

$$D = \begin{pmatrix} 1 & 6 & 2 \\ 6 & 3 & 8 \\ 2 & 8 & 2 \end{pmatrix} mod\ 17$$

Inserting a new participant: New users Alice and Bob want to join the key interchanging group [4]. Trent chooses public identifiers for each of them, for instance, k-element vectors IAlice, IBob in GF(p). At this step, private keys are computed by Trent:

g*Alice* = (D * I*Alice*), g*Bob* = (D * I*Bob*).

Each will employ their private key to calculate shared keys with other participants of the group.

$$I = \begin{pmatrix} 3 \\ 10 \\ 11 \end{pmatrix} \qquad I = \begin{pmatrix} 1 \\ 3 \\ 15 \end{pmatrix}$$

Let Alice , and Bob

Trent will produce Alice's and Bob's secret keys as follows:

$$g = \begin{pmatrix} 1 & 6 & 2 \\ 6 & 3 & 8 \\ 2 & 8 & 2 \end{pmatrix} \begin{pmatrix} 3 \\ 10 \\ 11 \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ 6 \end{pmatrix}$$

Alice * = mod 17

$$g = \begin{pmatrix} 1 & 6 & 2 \\ 6 & 3 & 8 \\ 2 & 8 & 2 \end{pmatrix} \begin{pmatrix} 1 \\ 3 \\ 15 \end{pmatrix} \begin{pmatrix} 15 \\ 16 \\ 5 \end{pmatrix} \text{mod } 17$$

Bob * =

Computing a shared key between Alice and Bob: At present, Alice and Bob request to communicate with one another. Alice has Bob's identifier; IBob and her private key gAlice. She determines the shared key:

$$k_{\text{Alice/Bob}} = g_{\text{Alice}}^{t} * I_{\text{Bob}}$$

Here, t indicates the matrix transpose. Bob does the equivalent task, using his private key and her identifier.

They will generate their shared key as follows:

$$k_{\text{Alice/Bob}} = \begin{pmatrix} 0 \\ 0 \\ 6 \end{pmatrix}^{t} * \begin{pmatrix} 1 \\ 3 \\ 15 \end{pmatrix} =$$

$$0 * 1 + 0 * 3 + 6 * 15 = 5 \bmod 17$$

$$k_{\text{Bob/Alice}} = \begin{pmatrix} 15 \\ 16 \\ 5 \end{pmatrix}^{t} * \begin{pmatrix} 3 \\ 10 \\ 11 \end{pmatrix} =$$

$$15 * 3 + 16 * 10 + 5 * 11 = 5 \bmod 17$$

Attack resistance: It's required to assure at least k compromised keys ahead of every shared key can be computed by an attacker. Therefore, identifiers must be k-linear autonomously; all k-sets of random selected user identifiers must be linear independently. Apart from that a group of malicious users can compute the key of any other member whose identifier is dependent to theirs linearly. To ensure this property, the identifiers shall be chosen from a MDS-Code matrix (maximum distances separable error correction code matrix) preferably. The rows of the MDS-Matrix demanded to be the identifiers of the users. A MDS-Code matrix can be elected using the code-matrix of the Reed–Solomon error correction code, practically. In this way, it can be computed very fast.

Results:

Implementation of the concept of this paper and different results is illustrated as follows. The proposed design is implemented in Java technology on an Intel ® Core i5-2450M CPU 2.50 GHz PC with 256 GB hard disk and 4 GB RAM with Java Environment. The propose paper's concepts show efficient results and have been efficiently tested on different data sets. Fig.4-10 present the result in different stages.

Conclusion:

In this procedure, end to end safe connections was investigated in haphazard of wireless sensor networks. This is performed via differentiated key pre-distribution, while distributing a distinct number of keys to various sensors is utilized. Therefore, high resilience of certain links within the network was obtained. This aspect is leveraged throughout routing, where node's route via links with higher resilience. End to end secure communication protocol was demonstrated according to the above methodology through developing justify location and data routing protocols.

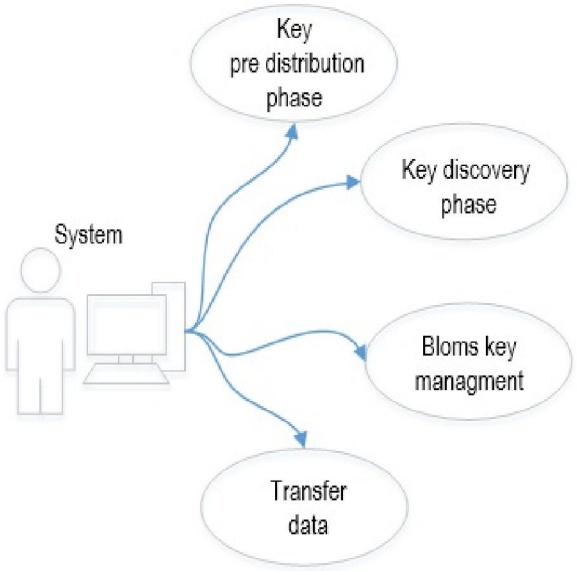

Fig. 1 User case diagram

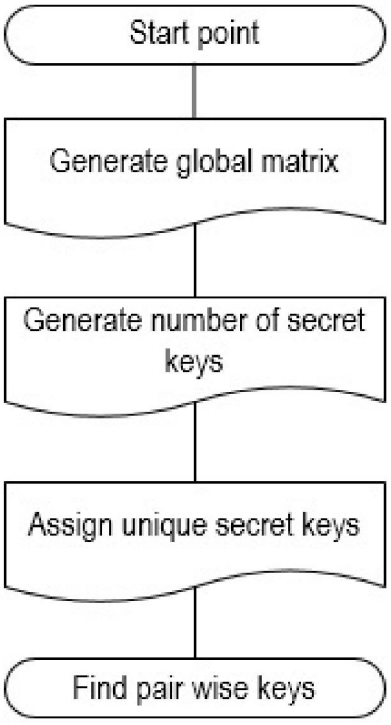

Fig. 2 Key pre distribution phase

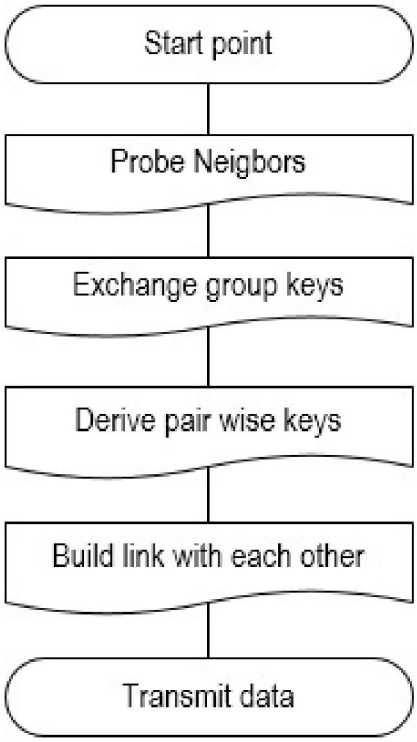

Fig. 3 Key discovery phase

Fig. 4 Assigning neighbor nodes and ports

Fig. 5 Produced random keys

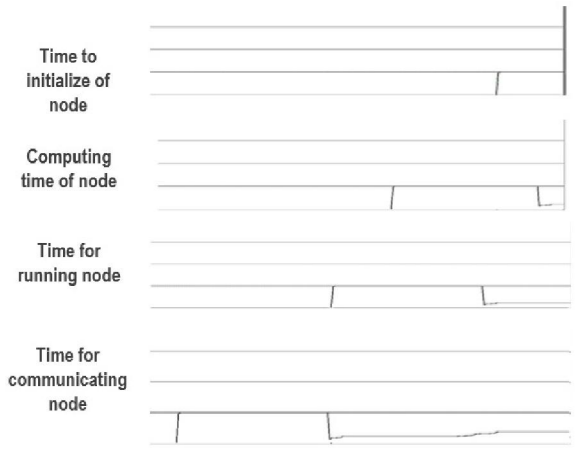

Fig. 6 Taken time by node in various steps

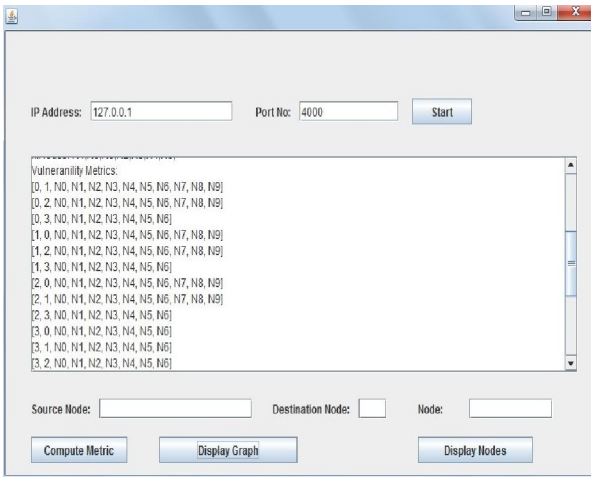

Fig.7 Node calculations

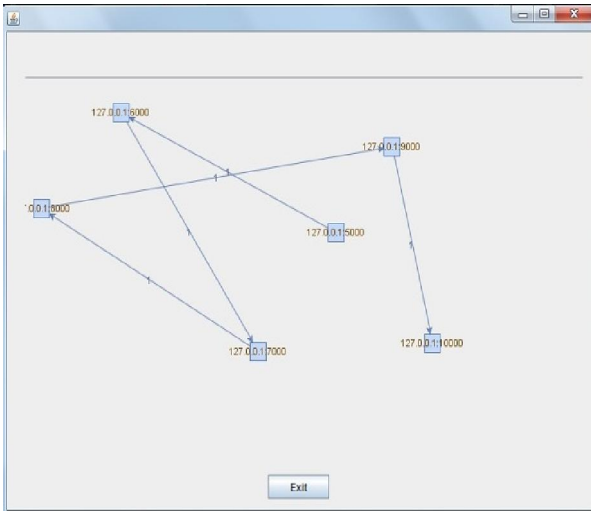

Fig. 8 Routing result with first random produced keys (six nodes)

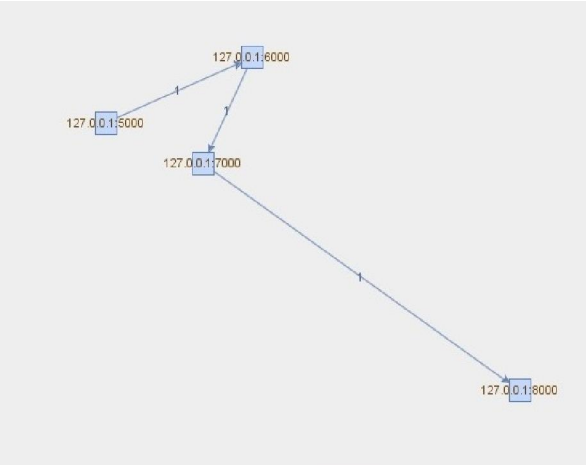

Fig. 9 routing result with second random produced keys (four nodes)

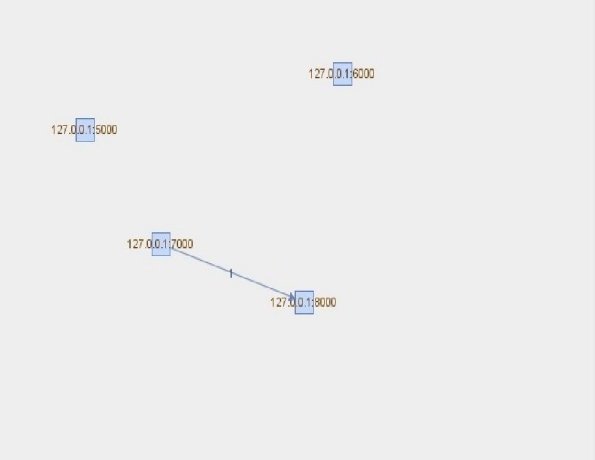

Fig. 10 Deletion of some routes

References:

1. H. Dai and H. Xu, "Triangle-based key management scheme for wireless sensor networks," *Frontiers Electrical Electron. Eng. China*, vol. 4, no. 3, pp. 300-306, 2009.
2. L. Eschenauer, V. D. Gligor, "A key-management scheme for distributed sensor networks," *Proceedings of the 9th ACM Conference on Computer and Communications Security (CCS '02),* pp. 41–47, 2002.
3. Poornima and B. Amberker, "Tree-based key management scheme for heterogeneous sensor networks," *in 16th IEEE International Conf. Netw*, 2008.
4. D. Liu and P. Ning, "Establishing pairwise keys in distributed sensor networks," *in proceedings of the 10th ACM conference on Computers and Communication Security (CCS'03),* pp.52-61, 2003.
5. Y. Zhang, W. Yang, K. Kim, and M. Park, "An AVL tree-based dynamic key management in hierarchical wireless sensor network," in *Proc. International Conf. Intelligent Inf. Hiding Multimedia Signal Process.*, pp. 298-303, 2008.
6. C. Ferreira, M. A. Vilac¸a, L. B. Oliveira, E. Habib, H.C. Wong, and A. A. F. Loureiro. "On the security of cluster based communication protocols for wireless sensor networks*", In 4th IEEE International Conference on Networking (ICN'05), volume 3420 of Lecture Notes in Computer Science, Reunion Island*, pp. 449–458, 2005.
7. S. Bandyopadhyay and E. J. Coyle, "An Energy Efficient Hierarchical Clustering Algo-rithm for Wireless Sensor Networks," *in Proceeding of IEEE INFOCOM'03, San Francisco*, 2003.
8. M. Eltoweissy, M. Moharrum and R. Mukkamala, "Dynamic key management in sensor networks," *IEEE Communications Magazine **44**(4)*, pp. 122–130, 2006.
9. W. Du et al., "A Key Management Scheme for Wireless Sensor Networks using Deployment Knowledge," *Proc. IEEE INFOCOM, Hong Kong*, pp. 586–97, 2004.
10. D. Liu and P. Ning, "Location-Based Pairwise Key Establishments for Static Sensor Networks," Proc. ACM Wksp. Security Ad Hoc and Sensor Networks, 2003.
11. Poornima and B. Amberker, "Key management schemes for secure communication in heterogeneous sensor networks," *International J. Recent Trends Eng.*, 2009.
12. H. Chan and A. Perrig. and D. Song," Random key pre distribution schemes for sensor networks," *IEEE symposium on Research in Security and Privacy*, pp.197-213, 2003.
13. S. Hussain, F. Kausar, and A. Masood, "An Efficient Key Distribution Scheme for Heterogeneous Sensor Networks," *IWCMC'07*, 2007.
14. R. D. Pietro, L. V. Mancini, and A. Mei, "Random Key assignment to secure wireless sensor networks," In 1st ACM workshop on Security of Ad Hoc and Sensor Networks, 2003.
15. Das, "An unconditionally secure key management scheme for large scale heterogeneous wireless sensor networks," in *Proc. First International Commun. Syst. Netw. Workshops*, pp. 1-10, 2009.
16. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks," *IEEE Communications Magazine,* Vol. 40, pp. 102-114, 2002.

17. Hwang and Y. Kim, "Revisiting random key pre distribution schemes for wireless sensor networks*," In 2nd ACM workshop on Security of ad hoc and sensor networks*, pp. 43-52, 2004.
18. Hartung, J. Balasalle and R. Han, "Node Compromise in Sensor Networks: The Need for Secure Systems," *Technical Report CU-CS-990-05*, 2005.
19. W. B. Heinzelman, A. P. Chandrakasan, and H. Balakrishnan, "An Application-Specific Protocol Architecture for Wireless Microsensor Networks," *IEEE Trans. Wireless Commun., Vol. 1, no.4*, pp. 660-670, 2002.
20. Y. Yang, J. Zhou, R. Deng, and F. Bao, "Hierarchical self-healing key distribution for heterogeneous wireless sensor networks," *Security Privacy Commun. Netw,* pp. 285-295, 2009.
21. Perrig, R Szewczyk, V Wen, D Culler, JD Tygar and SPINS "security protocols for sensor networks," *Proceedings of the 7th Annual International Conference on Mobile Computing and Networking*, pp. 189–199, 2001.
22. N. Al-Karaki and A. E. Kamal, "Routing Techniques in Wireless Sensor Networks: A Survey," *IEEE Wireless Commun., vol.11, no. 6*, pp. 6–28, 2004.
23. Y. Zhang, W. Liu, W. Lou and Y. Fang, "Location-based compromise-tolerant security mechanisms for wireless sensor networks," *IEEE Journal on Selected Areas in Communications **24**(2)*, pp. 247–260, 2006.
24. J. N. Al-Karaki and A. E. Kamal, "Routing Techniques in Wireless Sensor Networks: A Survey," *IEEE Wireless Commun., vol.11, no. 6*, pp. 6–28, 2004.
25. B. Tian, S. Han, and T. Dillon, "A key management scheme for heterogeneous sensor networks using keyed-hash chain," in *5th International Conf. Mobile Ad-hoc Sensor Netw.*, 2010.
26. J. Kim, J. Lee, and K. Rim, "Energy efficient key management protocol in wireless sensor networks," *International J. Security its Appl.*, 2010.
27. Wen, L. Dong, Y. F. Zheng and K. F. Chen, "Towards Provable Security for Data Transmission Protocols in Sensor Network," *Journal of Information Science and Engineering, Vol. 25, No. 1*, pp. 319-333, 2009.
28. Y. C. Zhang and Y. G. Fang, "ARSA: An Attack- Resilient Security Architecture for Multi-Hop Wireless Mesh Networks," *IEEE Journal on Selected Areas in Communications, Vol. 24, No. 10*, pp. 1916-1928, 2006.
29. D. Liu and P. Ning, "Establishing Pairwise Keys in Distributed Sensor Networks," *ACM Transactions on Information and System Security, Vol. 8, No. 1,* pp. 41-77, 2005.
30. W. Du, 1. Deng, Y. S. Han, S. Chen, and P. K. Varshney, "A key management scheme for wireless sensor networks using deployment knowledge," in 23rd Conference of the IEEE Communications Society (Infocom 04), Hong Kong, China, March 21-25, 2004.
31. H. Jen-Yan, I. Liao, and H. Tang, "A forward authentication key management scheme for heterogeneous sensor networks," *EURASIP J. Wireless Commun. Netw,* 2010.
32. G. Jolly, M. C. Kuscu, P. Kokate, and M. Younis, "A low-energy key management protocol for wireless sensor networks," *Proceedings of the 8th IEEE international Symposium on Computers and Communications*, pp.335–340, 2003.
33. Wen, Z. Yin, Y. Long, and Y. Wang, "An adaptive key management framework for the wireless mesh and sensor networks," *Wireless Sensor Netw. J.*, 2010.
34. H. Chan, A. Perrig and D. Song, "Random key pre distribution schemes for sensor networks," *Proceedings of the IEEE Symposium on Security And Privacy*, pp.197–213, 2003.
35. L. D G and N. P, "Establishing pairwise keys in distributed sensor networks," *in Proceedings of the 10th ACM Conference on Compute and Communications Security. New York: ACM*, pp.52–61, 2003.
36. Y. Kumar, R. Munjal and K. Kumar, "Wireless Sensor Networks and Security Challenges," *IJCA Proceedings on National Workshop-Cum-Conference on Recent Trends in Mathematics and Computing 2011 RTMC(9), Published by Foundation of Computer Science, New York, USA*, 2012.
37. X. Chen, K. Makki, K. Yen, and N. Pissinou, "Sensor Network Security: A Survey", *IEEE Communications Surveys & Tutorials, vol. 11, no. 2,* pp. 52-62, 2009.
38. C. Karlof and D. Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures", *Ad Hoc Networks (elsevier),* pp. 299-302, 2003.

Author's profile:

Ahmad Sharifi. He has received his M. Tech in Computer Networks and Information Security from Jawaharlal Nehru Technological University (JNTU), Hyderabad, India. In addition, he has received his Bachelor in Electronic engineering from industrial university of Shahrood, Iran. Ahmad has professional experiences on technical engineering on ISP and network designs for many years. In addition, he is involving with teaching in universities as well as Cisco training performances. He is interested in Cryptography, WSN, ADHOC, MATLAB, OPNET and other related issues. His personal website is www.ahmadsharifi.com. Furthermore, he cooperates with RIPE NCC www.ripe.net via www.sharifisdp.com that is an Internet Service Provider.

Mohsen Khosravi. He is a PhD student in the Information Technology department of Information and Communication Technology (KICT) of International Islamic University Malaysia (IIUM). He has received his Master of Information Technology from Jawaharlal Nehru Technological University (JNTU), Hyderabad, India. His bachelor is software engineering from Azad university of Lahijan, Iran. His fields of interests are ADHOC, WSN and RFID that he works on it specially.

Hasan Sharifi. He has received his degree in Management from PNU University, Iran. He is studying MBA in Azad Shahrood University, Iran. And he has obtained special courses in MBA and marketing regarding experiences. In addition, he has worked for many years in IT management, quality of service (QOS), hardware and network topologies including ADSL2+, Wireless LANs for different companies and consumers. Hassan works as technical and planning engineer for http://www.sharifisdp.com that is also a RIPE NCC member http://www.ripe.net

Jallaledin Sharifi. He is a Microsoft engineer. He has obtained MCITP 2008, besides of other experts and certificates in Cisco Technologies, MikroTik Routers and wireless, Linux based servers, WLAN, IPV4 and IPV6. In addition, he is chief of Sharif Network Designers Company http://www.sharifisdp.com that includes Internet Service Providing and Distribution of services to consumers. Also he is a member of RIPE NCC http://www.ripe.net. Network topologies and infrastructure to the best quality of service in IT domain are considered as his professions. He designs for performance of modern services to enterprises.

2/1/2016