A Survey on Security Techniques in Group Communication for Wireless Sensor Networks

H S Annapurna
Research Scholar,
Sri Siddhartha Institute of Technology,
Tumkur, India

M. Siddappa, Ph.D.
Professor and Head,
Dept. of Computer Science and Engg.
Sri Siddhartha Institute of Technology, Tumkur,
India

ABSTRACT

A wireless network is a type of network where various physical devices (e.g. computer, laptops, PDAs etc) are interconnected with each other using network infrastructure. Owing to wireless medium of data communication, the security risk is potentially high for unauthorized access and intrusion of various malicious programs. The security protocols of wireless network are governed by family of IEEE 802.11 standards. Wireless Network is studied in research with respect to wireless LAN (Local Area Network), wireless mesh network, wireless sensor network, mobile adhoc network, etc. In recent times, wireless sensor network was on constant focus among the research community owing to its potential advantage of data collection in remote areas as well as security problems associated with it. Wireless Sensor Network (WSN) consists of various sensor motes that form a cluster and perform data aggregation. Usually, the aggregated data is forwarded from the sensor nodes to the base station, which then reaches to user for analysis. The security problems is a matter of concern even for wireless sensor network that aims for either compromising the routing protocols or invoke illegitimate access to resources by bypassing the security protocols. In a wireless sensor network, the communnunication takes place by group based, where sensor nodes are deployed in groups and each group performs communication using keys. Therefore this paper reviews some of the potential key-management techniques in past for maintaining group based communication and extracts the research gap.

Keywords

Application Dependent Sensor Network, Key Management, Security, WSN

1. INTRODUCTION

A wireless network is type of network that connects various computing devices (server machines, client machines) along with other hardware (printers). This is the best cost-effective alternative for wired network that ensure better reachability and extremely less maintenance issues. Some of the distinguished example of wireless network includes mobile adhoc network, Wireless Local Area Network (WLAN), and terrestrial microwave networks. Wireless Network are broadly classified as Wireless personal area network (WPAN), Wireless Local Area Network (WLAN), Wireless Mesh Network, Wireless Metropolitan Area Network (WMAN), Wireless Wide Area Network (WWAN), Cellular network, Wireless Sensor Network, Mobile Adhoc network, WiMax, etc. Wireless Sensor Network (WSN) comprises of sensor nodes that are interconnected with each other to perform data aggregation. The sensor node is a device that can perceive the physical attributes of the environment e.g. heat, pressure, moisture, motion, smoke, etc. The various application of WSN is actually based on the functionalities of node [1] [2]. Security is an important area of research even before the introduction of WSN. Reliable security mechanisms like Diffie-Hellman key exchange algorithm [3], RSA [4], TLS [5] and Kerberos [6] existed even before the introduction of WSN. However, these protocols did not consider resource constraints as an important issue. Along with minimizing the resource usage, confidentiality, integrity, availability and authenticity should be maintained in all types of WSN. In order to compromise confidentiality, integrity, availability and authentication of a network, adversary can adopt different attack strategies. However, not all attack strategies are applicable in all types of WSNs. Key management is the most important part of WSN security. Apart from maintaining confidentiality, it also assists other modules such as authentication, privacy and sometimes integrity. Therefore it is important to have key management strategy, which provides security as per the requirements of target WSN application and also incurs lesser overhead on sensor nodes. A group based communication system in WSN usually consists of multiple groups, where each group consists of certain number of sensor nodes. In order to perform communication, group based communication system totally depends on efficient key management or exchange system that finally ensure the security while performing communication among the multiple groups. Hence, it is necessary that key-management techniques presented by various literatures applied over group based communication system be studied. It is primarily essential as WSN is vulnerable toward multiple threat scenarios (or an attack) that disrupts the group based communication system. Hence, the proposed review paper aims to discuss all the possible threat scenarios as well as available key management techniques. The objective of the paper is to discuss about the threats and the key management schemes in WSN and to provide the quantitative comparison of the prominent key management schemes in each scenario of WSN.

2. RECENT STUDIES

Kausar et al. [7] have proposed an approach for securely distributing rekeying messages and identified techniques for fusion and parting a group. The authors have also presented a self-healing key distribution plan for protecting multicast group communications for WSN. Gaddour et al. [8] have proposed a framework to bound the access to the group data completely to the members that have securely joined the group. The major contributions of the work was (1) a proficient and secure group management mechanism for cluster-tree networks, and (2) a secure key allotment between group members. Garcia et al. [9] have presented a secure group-based architecture for WSNs. The sensor network presented has two security zones. On the one hand there was an intra-group security and, on the other hand, the intergroup security. Tian et al. [10] proposed involuntary healing key distribution schemes to address packet loss issues. The authors have presented mutual-healing key distribution plan that depend on bilinear pairings. The method is collusion-free for several coalitions of non-authorized nodes. Every node's private key has nothing to do with the number of retracted nodes and may be reclaimed as long as it is not revealed. The storage space transparency for every node is found to be stable. Cheikhrouhou et al. [11] have proposed a novel secure group management method with an insubstantial re-keying process. The methods permit multiple logical groups; every group is maintained and rekeyed disjointedly by a resource-constrained sensor node without requiring much multicast routing. The authors have discussed that the method is secure. Cheikhrouhou et al. [12] have proposed a method that depends on a logical ring design, which allows improving the group controller's task in revising the group key. The method also presents backward and forward secrecy, concentrating on the node cooperation attack, and gives a clarification to detect and abolish the cooperation's nodes. Nicanfar and Leung [13] have illustrated a group-key management method focused at securing the group communications. The method is depend on the X.1035 Password Authenticated Key Exchange protocol typical, and also tracks the cluster based loom to decrease the costs of the group key production and preservation for large groups. Bechkit et al. [14] have demonstrated an improved until-depend key pre-distribution method presenting high network scalability and high-quality key sharing prospect. The attained results demonstrate that their approach improves significantly the network scalability even as providing high secure connectivity expositing and good generally presentations. Bag and Roy [15] have presented a key predistribution method in a grid-group exploitation of sensor nodes. The method makes sure that there will be high probability of survival of an ordinary unexposed link between two nodes belonging to two dissimilar groups yet if a substantial number of nodes are cooperation's by the opponent. Sahoo and Sahoo [16] have illustrated an elliptic curve depends hierarchical cluster key management method, which is extremely secure, have enhance time difficulty and guzzles reasonable quantity of energy.

3. THREAT POSSIBILITIES IN WSN TOPOLOGIES

In this section, the threat possibilities in WSN causing potential damage to the group communications are identified [7].

- **DoS (Denial of Service) Attacks**: Denial of service attacks is carried out with the help of an outsider node, which disrupts the communication channel between the communicating sensor nodes. Jamming attack is a type of DoS attack.

- **Passive Information Gathering and Message Corruption**: In these attacks, adversary listens to the information passively. It can also try to corrupt the messages being exchanged between different nodes.

- **Node Compromise**: An adversary can exploit a hole in the system software of a sensor node to gain control of the node. Compromised node can listen to the communication between other nodes, interrupt communications, intercept messages, modify and fabricate messages.

- **Node Tampering**: In this case, an adversary gets hold of a sensor node physically and gains access to all data, information and important cryptographic material. When a node is tampered, it is compromised physically and it can be used to listen to communications, interrupt them, intercept, modify and fabricate messages.

- **False Node**: In this case, an illegitimate node is introduced in a sensor network. It tries to act as a legitimate node, tries to inject false data in the network or tries to attract data towards itself.

- **Node Outage**: In node outage attack, adversary removes the node from the network or drains all its energy.

- **Traffic Analysis**: Adversary can passively analyze the traffic patterns in a sensor network. This can lead to a calculated attack on a sensor network.

- **Acknowledgment Spoofing**: An attacker node can spoof the acknowledgment of a data packet, which has not been transferred to the receiver successfully. This hampers the information from getting to the sink node. Either, the receiver node is dead, or it is barred from receiving the data packet in some other way.

- **Spoofed, Altered or Replayed Routing Information**: A compromised node is used to play with the routing information and disseminate false routing information through a sensor network.

- **Selective Forwarding**: A false or compromised node is used to create a black hole in the target sensor network. False or compromised node deliberately drops data packets to disrupt network operation.

- **Sinkhole Attacks**: This is similar to selective forwarding except that it is not a passive attack. In this case, traffic is attracted towards the compromised or false node.

- **Sybil Attacks**: In Sybil attacks, malicious node presents multiple identities to the sensor network either by creating them or by stealing the identities of other nodes.

- **Wormhole Attacks**: Two distant malicious nodes are used to create a wormhole in the target sensor network. Both malicious nodes have an out of band communication channel. One node is placed near the sensor nodes. It advertises shortest path to the sink node through the other one, which is placed near the sink node. This creates sinkholes and routing confusions in the target sensor network.

- **Hello Flood Attacks**: In hello flood attack, a malicious node plays or replays a hello packet with high signal strength in the target sensor network. High signal strength makes all other nodes think that the malicious node is their neighbor. It then creates a wormhole. Also, other sensor nodes lose their energy in replying to the hello packet.

4. KEY MANAGEMENT SCHEMES

The different key management schemes frequently adopted for group communication system in WSN are discussed in this section [8]:

4.1 Single Network-Wide Key

This type of scheme permits the entire sensor node to store a single key to perform secure communication. The first advantage of using single key system is minimal overhead for performing secured group communication. The second advantage is minimal storage overhead owing to less extent of computation involved. The prominent disadvantage of this scheme is if any one sensor node is compromised, the single key stored is compromised too very easily. The scheme is also highly vulnerable towards majority of cryptanalytic attacks.

4.2 Pair wise Key Organization

This type of key management techniques calls for using a pair of key with all the sensor nodes present in the network. The advantage of using this key scheme is less communication and computation overhead but disadvantage is extreme overhead on storage. Although pairwise key management ensures better security, but it doesn’t ensure optimal scalability.

4.3 Random Pair-Wise Key Establishment

The random pairwise key management scheme was mainly designed to cover up the potential loopholes in conventional pairwise key management scheme [9]. This scheme is based on the fact that all the sensor nodes will not be required to perform communication among them. A sensor node shares a common secret key with a certain probability for retaining the optimally required network connectivity. The scheme introduced in [9] discusses that if any one node in the network senses the vulnerability, than they abort all the communication with that specific sensor node. The scheme renders the compromised sensor node to overhead any sorts of ongoing communication

4.4 Trusted Key Distribution Center (KDC)

Pair-wise key management schemes are based on trusted key distribution center to introduce mechanisms for node authentication. Inside pair wise key organization methods, pair wise keys is already loaded on the sensor nodes and neighboring sensor nodes start communication with each other directly. In this method, each and every pair-wise key are accumulates on a conviction server. This server can be the base station or a sensor node. Every pair of nodes contacts the trusted node to obtain a pair-wise key for every session. This scheme is resilient against node capture and node replication. However, there are many drawbacks of this scheme. This scheme imposes high communication overhead, high storage overhead on the trusted node and can cause congestion on the links around the trusted node. In addition to that, the scheme also requires the trusted node to have more capabilities than other sensor nodes and it causes the trusted node to become a single point of failure for the network. This scheme is certainly not suitable for sensor networks having large number of nodes.

4.5 Random Key Pre-distribution Scheme

In random key pre-distribution scheme [10], a key-chain is stored in every sensor node. All keys are called as group keys, which the base station shares with a group of sensor nodes. Upon deployment, every sensor node can only communicate with those sensor nodes, with which it shares a secret key. Also, if a node has a redundant key after network initialization, it can use that key to establish communication path between two other nodes, which do not share a common key. If a node is compromised, the base station broadcasts the list of keys that it possesses. All other nodes delete these keys from their memories. A significant drawback of this scheme is that communication links that are not directly related to the compromised nodes are also affected. Although efficiency of random key pre-distribution scheme can be argued, but it is equally applicable to all static sensor networks.

4.6 Q-Composite Random Key Pre-distribution Scheme

In order to cater up for the drawback of random key pre-distribution scheme, Q-Composite random key pre-distribution scheme was proposed [9]. In this case, if two sensor nodes need to communicate with each other, they must share at least *q* number of keys. When a compromised node is evicted and its keys are revoked, other links remain unaffected. However, the key pool is reduced to maintain the probability that two nodes share *q* common keys. So, the adversary would need to compromise a few nodes to compromise the whole network.

4.7 Multi-path Key Reinforcement Scheme

In multi-path key reinforcement scheme, multiple paths are established between two communicating nodes [9]. As an example, consider that two nodes *A* and *B* have *h* disjointed paths between them and they use key *k* for communication. One node sends h different random values to the other node through separate paths. Then they both compute a key *k’* using key *k* and *h* random values. If key *k* is compromised, they refresh it using k’. This scheme increases the computation overhead of sensor nodes, which drains precious energy. For unlimited energy, static sensor networks, this scheme is better than random key pre-distribution and Q-composite random key pre-distribution schemes because of increased security.

4.8 Polynomial Pool-based Key Pre-Distribution

In this case, one *t* degree polynomial is assigned to each sensor node [11]. The polynomial has a property that *f(x, y) = f(y, x).* If nodes *i* and *j* receive polynomials *f(i y)* and *f(j, y)* respectively, they can compute a common key using identity of the other node. This is a scalable scheme but whole network is compromised if t nodes are compromised. This scheme suits large-scale sensor networks because of its scalability and dynamic sensor networks because of its ability to establish connection with unknown sensor nodes.

4.9 Public Key Cryptography in WSN

Public Key Cryptography schemes require highly sophisticated computation, which consumes precious energy from sensor nodes. Most researchers argue that public key cryptography should not be employs in wireless sensor networks (WSNs) since of extreme computation costs. However, some researchers argue that public key cryptography especially Elliptic Curve Cryptography (ECC) cannot be ruled out of WSNs [12], [13], [14]. According to [12], 160-bit ECC provides the same level of security as found in 1024-bit RSA [4] and the difference in the number of bits is exponential because 224-bit ECC provides same level of security as 2048-bit RSA. Hybrid approaches have also been proposed for WSN. In hybrid approaches, both symmetric and asymmetric keys are used [15]. Public key cryptography is not viable to use in those sensor networks, which have large number of nodes. It is viable for sensor networks, having small number of nodes especially if they fall under the category of unlimited energy static sensor networks.

4.10 SHELL

SHELL scheme is designed for large scale clustered sensor networks. SHELL makes use of EBS matrix to control a large number of nodes using a small number of keys. SHELL supports in-network- processing [17], [18] and avoids single point-of-failure in a network by involving cluster heads nodes of neighboring clusters for key management. An EBS system of matrices stores information about keys stored on every node. There are a total of $k + m$ keys, out of which every node knows a distinct set of k keys. If a node is compromised, m keys, which are not known to the compromised node, are used to refresh the k compromised keys to evict the compromised node. Total number distinct sets of k keys can be depicted by this formula: -

$$\eta = \frac{(k+m)!}{k!m!} \tag{1}$$

SHELL is an ideal key management scheme for High Density, Static Sensor Networks. Also, it is a very viable solution for those High Density, Dynamic Sensor Networks, in which node mobility is low i.e., within the area of a defined cluster. This is a workable but not efficient solution for other classes of sensor networks like Energy Constrained, Low Density, and Static Sensor Networks, Unlimited Energy, Static Sensor Networks and Low Density, Dynamic Sensor Networks. For Wireless Body Area Networks, this solution is not always usable because Wireless Body Area Networks does not necessarily have neighboring clusters. Also, number of nodes is very small in Wireless Body Area Networks.

4.11 MUQAMI+

MUQAMI+ is also an EBS based key management scheme for large scale clustered sensor networks [19]. In this scheme, responsibility of key management is distributed within the same cluster and inter-cluster communication is avoided. Also, computation and storage overhead is reduced. Single point of failure is avoided by distributing the responsibility of key management among a small fraction of nodes within the cluster. This is done with the help of one-way hashing [20] functions and key-chains [21]. Although the CH node stores the EBS matrix, it does not get to know the actual key values. Even in the case of node compromise, messages are sent through the CH node but the key values are not revealed to it in order to maintain the property of not having a single point of failure in a cluster. Also, responsibility of being cluster head node or generating keys can be shifted from one node to another with minimal overhead.

4.12 LEAP+

LEAP+ [22] is a key management solution that is not targeted towards some specific class of sensor networks. In LEAP+, each node's cluster consists of all its neighbors. In this scheme, every node stores 4 types of keys. One key is shared with the base station. After deployment, every node establishes keys with all its neighbors. After that, it shares another key with all is neighbors for broadcast purposes. Finally, there is a single network-wide key used for broadcast purposes in the whole network. If a node is compromised, its neighboring nodes delete pair-wise keys shared with it, and then refresh their group keys, which they use for broadcast purposes. In the end, network-wide key is refreshed. LEAP+ is a key management solution that is equally applicable to almost all classes of static sensor networks. It is ideal for use in energy constrained, low density, static sensor networks and unlimited energy, static sensor networks. Also, it is a very scalable key management scheme and is useful for high density, static sensor networks. However, it is not suitable for wireless body area networks and not applicable in dynamic sensor networks.

4.13 Plug’s Play Key Management for Wireless Body Area Network

In the discussion up till now, we have seen that the applicability of any key management scheme in Wireless Body Area Network is different from its applicability in other classes of sensor networks. This is mainly because of the topology and scale of Wireless Body Area Network. From topology and scale, Wireless Body Area Network resembles Wireless Personal Area Network. However, Wireless Body Area Network is used to measure biometrics from human body, which has an effect on communication between sensor nodes planted on human body. Also, biometrics from human body exhibits certain randomness properties, which help in key management [23]. Falck et al. [24] proposed a solution for key management in Wireless Body Area Network based on the above mentioned research and studies. They proposed that the communicating sensor nodes do not even need to exchange keys in order to establish a communication link. In this scheme, two sensor nodes sense the same biometric at a particular time instant and then use error correcting codes to compute final key values. Error correcting codes remove the possible differences that may arise in the readings of the two nodes. This key management scheme is specifically designed for Wireless Body Area Network and is not applicable to other classes of WSNs. Although it is designed for specifically for Wireless Body Area Network, it is a primitive scheme and has many shortcomings.

4.14 BARI

BARI [25] covers the shortcomings of the existing key management solutions for Wireless Body Area Network. Apart from time synchronization and other issues in error correcting codes, two sensor nodes are supposed to sense a single biometric in [24]. This is not always possible because a patient any other human being might refuse to wear more than a certain number of devices. Also, one device is used to measure one biometric most of the time. Devices, measuring multiple biometrics might have financial implications. In BARI, it is assumed that a small number of nodes are placed on human body and each nodes senses its own biometric. The base station, also called the personal server, issues a key refreshment schedule. Every node refreshes the key on its turn. When all nodes have taken their turn, new refreshment schedule is issued by the base station. Even though node compromise is not very common in such indoor human attended environments, BARI has a provision for evicting compromised nodes. BARI is designed specifically for Wireless Body area network environments.

5. COMPARATIVE STUDY

The analysis of the proposed study is done by considering 6 classes of the applications in WSN e.g. i) *Class-1*: High density, static sensor networks, ii) *Class-II*: High density, dynamic sensor networks, iii) *Class-III*: Energy constrained, low density, static sensor networks, iv) *Class-IV*: Unlimited energy, static sensor networks, v) *Class-V*: Low density, dynamic sensor networks, vi) *Class-VI*: Wireless body area networks. The applicability of every key management technique in each scenario of in WSN is summarized in

Table I. It is assumed that for a scheme to be applicable in dynamic WSN, it should be able to accommodate high node mobility.

Apart from only being able to provide basic protection i.e. help in maintaining confidentiality and integrity of information and authenticating the users through secret keys, a key management scheme should be able to refresh keys in a secure way and evict malicious nodes from the network whenever necessary. A key management scheme may be more energy efficient as compared to other schemes but provide less security services as compared to other schemes. Therefore, it is important to compare the security services provided by each key management scheme. The comparison of the services provided by each key management scheme discussed in this paper is shown in Table II. When deciding an appropriate key management scheme for any scenario of WSN, it is important to choose a scheme that provides maximum security services. After that, we should focus on efficiency.

Table I. Applicability of Every Key Management Scheme in Each Scenario of WSN

Scheme	Class-I	Class-II	Class-III	Class-IV	Class-V	Class-VI
Single Network-wide Key	Yes	Yes	Yes	Yes	Yes	Yes
Pair-wise Key Establishment	No	No	Yes	Yes	Yes	Yes
Random Pair-wise Key Establishment	No	No	Yes	Yes	Yes	Yes
Trusted Key Distribution Center (KDC)	No	No	Yes	Yes	Yes	No
Random Key Pre-Distribution	Yes	Yes	Yes	Yes	Yes	No
Q-Composite Random Key Predistribution	Yes	Yes	Yes	Yes	Yes	No
Multi-path Key Rein-Forcemeat	Yes	No	Yes	Yes	No	No
Polynomial Pool-based Key Pre-Distribution	Yes	Yes	Yes	Yes	Yes	No
Public Key Cryptography	No	Yes	Yes	Yes	Yes	No
SHELL	Yes	No	Yes	Yes	No	No
MUQAMI+	Yes	No	Yes	Yes	No	Yes
LEAP+	Yes	No	Yes	Yes	No	Yes
Plug 'n Play Key Management for Wireless Body Area Networks	No	No	No	No	No	Yes
BARI	No	No	No	Yes	No	Yes

Table II. Comparison of Services Provided by Each Key Management Scheme

Scheme	Basic Protection	Key Refreshment	Node Eviction
Single Network- wide Key	Yes	No	No
Pair-wise Key Establishment	Yes	No	No
Random Pair-wise Key Establishment	Yes	No	No
Trusted Key Distribution Center (KDC)	Yes	Yes	Yes
Random Key Pre-Distribution	Yes	No	No
Q-Composite Random Key Predistribution	Yes	No	No
Multi-path Key Rein-For cement	Yes	Yes	No
Polynomial Pool-based Key Pre-Distribution	Yes	No	Yes
Public Key Cryptography	Yes	Yes	No
SHELL	Yes	Yes	Yes
MUQAMI+	Yes	Yes	Yes
LEAP+	Yes	Yes	Yes
Plug 'n Play Key Management for wireless body area Networks	Yes	Yes	No
BARI	Yes	Yes	Yes

6. RESEARCH GAP

Security in WSNs has attracted several research studies that have addressed various security problems such as authentication, key distribution, data confidentiality and integrity, intrusion detection, secure broadcast, and cryptography. The security problem in WSNs became even more challenging when dealing with the group security, as this grouping impose additional overhead in terms of network management. Several works have also addressed the latter problem; however, each of them relies on a specific and different grouping concept. In this paper, we focus on securing group communications in cluster-tree WSNs, where a collection is distinct as a place of sensor nodes sharing common private information. This means that sensor nodes in a given group must send and receive messages to/from group members in a way that outsiders are unable to unveil the shared group data, even when they are able to intercept the broadcasted messages. Thus, the main challenges can be summarized as follows: (1) the initiation and distribution of a group key in a secure and efficient manner, (2) the management of the group in the cluster-tree network. Keys are stored in nodes such that nodes in the same or neighboring groups have common keys, but nodes in distant groups do not share any. The literature was also found with techniques to form groups of sensor nodes with similar properties. However, this grouping concept is limited to sensor nodes located in a small region as a group is created in a region where an event is activated and sensors are combined together based on the defined properties. Many papers have discussed the key distribution problem in the context of group communication in WSNs. Various authors have also proposed an energy-efficient and level-based hierarchical system for WSNs, which also includes a group key management scheme which contains group communication policies, group membership requirements and an algorithm to generate a distributed group key. The frequently used group rekeying scheme requires many exponentially-complex operations, which turns it unpractical for large scale sensor networks. The existing authors addresses the problems of key establishment in hierarchical sensor networks. All the researchers proposed a group-based key pre-distribution scheme based on hierarchical WSNs using vicariate polynomials and proposed to establish inter group and intra group keys. However, they consider groups with members that are in the same communication range.

7. CONCLUSION AND FUTURE WORK

There are many applications, for which sensor networks are deployed. It is important to identify different application areas so that researchers can focus on achieving efficient solutions for all types of sensor networks. We have identified WSN applications, then classified sensor networks into different classes and identified security attacks that can take place in each class of sensor networks. In the end, we discussed prominent key management schemes for WSNs and their applicability in each class of WSNs. Also, we provided the quantitative comparison of the prominent key management schemes in each scenario. Key Management schemes are important because they provide defense against attacks. However, it is equally important to research about attack detection mechanisms for WSNs. Our future research intends to implement key management scheme for secure group communication in WSN. A mathematical modeling will be designed for secure group communication using multi-tier key distribution scheme. This framework would be designed to generate pair wise key to perform key predistribution as well as key allocation at the sink. An algorithm will be designed where a specific size of keys will be chosen from a key pool for formulating a unique pair wise key between the multiple nodes (intermediate) that ensures secure group communication in WSN.

8. REFERENCES

[1] Tilak, Sameer, Nael B. Abu-Ghazaleh, and Heinzelman, W.2002. Taxonomy of wireless micro-sensor network models. ACM SIGMOBILE Mobile Computing and Communications Review, Vol. 6, No. 2, pp.28-36.

[2] Akyildiz, Ian F., Weilian Su, Yogesh Sankarasubramaniam, and Erdal Cayirci.2002.Wireless sensor networks: a survey. Computer networks, Vol. 38, No. 4, pp.393-422

[3] Diffie, Whitfield, and Hellman, Martin E.1976. New directions in cryptography. Information Theory, IEEE Transactions, Vol.22, No. 6, pp.644-654.

[4] Rivest, Ronald L., Adi Shamir, and Len Adleman.1978.A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM, Vol.21, No. 2, pp.120-126

[5] Allen, Christopher, and Tim Dierks. 1999. The TLS protocol version 1.0.

[6] Kohl, John T., B. Clifford Neuman, and Y. Theodore.1994. The evolution of the Kerberos authentication service.

[7] Kausar. F, Hussain. S, Park. J. H, and Masood. A.2007. Secure Group Communication with Self-healing and Rekeying in Wireless Sensor Networks. Springer-Verlag Berlin Heidelberg, pp. 737–748

[8] Gaddour, O., Koubaa, A., Abid, M.2009. SeGCom: A Secure Group Communication Mechanism in Cluster-Tree Wireless Sensor Networks. IEEE First International Conference on Communications and Networking, pp.1-7

[9] Garcia, M., Lloret, J., Sendra, S. and Lacuesta, R.2010. Secure Communications in Group-based Wireless Sensor Networks. International Journal of Communication Networks and Information Security, Vol. 2, No. 1

[10] Tian, B., Han, S., Hub, J., Dillon, T.2011. A mutual-healing key distribution scheme in wireless sensor networks. Journal of Network and Computer Applications, Elsevier, Vol.34, pp.80–88

[11] Cheikhrouhoua, O., Koubaab, A., Dinif, G., Alzaidd, H., Abid, M.2011. LNT: a Logical Neighbor Tree for Secure Group Management in Wireless Sensor Networks. The 2nd International Conference on Ambient Systems, Networks and Technologies (ANT), ScienceDirect, Elsevier, Vol.5, pp.198–207

[12] Cheikhrouhou, O., Koubaa, A., Dini, G., Abid, M.2011. RiSeG: a ring based secure group communication protocol for resource-constrained wireless sensor networks. Journal Personal and Ubiquitous Computing, ACM Digital Library, Vol.15, Iss.8, pp.783-797

[13] Nicanfar, H., and Leung, V.C.M.2012.Password Authenticated Cluster-Based Group-Key Agreement for Smart Grid Communication. Security and Communication Networks Security Comm. Networks, pp.1–11

[14] Bechkit, W., Challal, Y., Bouabdallah, A., and Tarokh, V.2013. A Highly Scalable Key Pre-distribution Scheme for Wireless Sensor Networks. IEEE Transactions on Wireless Communications, vol. 12, Iss. 2, pp.948-959

[15] Bag, S., and Roy, B.2013. A new key predistribution scheme for general and grid-group deployment of wireless sensor networks. EURASIP Journal on Wireless Communications and Networking

[16] Sahoo, S. K., and Sahoo, M. N.2014. An Elliptic Curve based Hierarchical Cluster Key Management in Wireless Sensor Network. Springer

[17] Eltoweissy, Mohamed, M. Hossain Heydari, Linda Morales, and I. Hal Sudborough.2006. Location-Aware Combinatorial Key Management Scheme for Clustered Sensor Network. IEEE Transactions on Parallel and Distributed Systems (TPDS), Vol.17,pp.865-882

[18] Madden, Samuel, Robert Szewczyk, Michael J. Franklin, and David Culler.2002. Supporting aggregate queries over ad-hoc wireless sensor networks. In Mobile Computing Systems and Applications, Proceedings Fourth IEEE Workshop on, pp. 49-

[19] Raazi, SMK-u-R., Sungyoung Lee, Young-Koo Lee, and Heejo Lee.2007. MUQAMI: A Locally Distributed key Management Scheme for Clustered Sensor Networks. IFIP International Federation for Information Processing, Vol.238, Springer, pp.333-348

[20] Lamport, Leslie.1981. Password authentication with insecure communication. Communications of the ACM, Vol. 24, No. 11, pp.770-772

[21] Dini, Gianluca, and Ida Maria Savino.2006. An efficient key revocation protocol for wireless sensor networks. In Proceedings of the International Symposium on World of Wireless, Mobile and Multimedia Networks, pp. 450-452

[22] Zhu, Sencun, Sanjeev Setia, and Sushil Jajodia.2006. LEAP+: Efficient security mechanisms for large-scale distributed sensor networks. ACM Transactions on Sensor Networks (TOSN), Vol. 2, No. 4, pp. 500-528

[23] Cherukuri, Sriram, Krishna K. Venkatasubramanian, and Sandeep KS Gupta.2003. BioSec: A biometric based approach for securing communication in wireless networks of biosensors implanted in the human body. In Parallel Processing Workshops, 2003. Proceedings. International Conference, pp. 432-439

[24] Falck, Thomas, Heribert Baldus, Javier Espina, and Karin Klabunde.2007. Plug'n play simplicity for wireless medical body sensors. Mobile Networks and Applications, Vol. 12, No. 2-3, pp.143-153.

[25] Raazi, SMK-u-R., Sungyoung Lee, Young-Koo Lee, and Heejo Lee.2009. BARI: A distributed key management approach for wireless body area networks. In Computational Intelligence and Security. CIS'09. International Conference, Vol. 2, pp. 324-329