Group Key Management Technique based on Logic- Key Tree in the Field of Wireless Sensor Network

Jyothi Metan
Research Scholar
Visvesvaraya Technological University,
Belgaum, India

K N Narasimha Murthy, PhD
Professor & Head (PG) Department of CSE
Vemana Institute of Technology,
Bangalore, India

ABSTRACT

In the recent times the concept of group key management is found to be one of the very essential issues in the field of wireless sensor network. Because of the dual impact limitations and various operations in open and hash environment the security and confidentiality which are considered as very challenging issues in WSN. The main issues which are associated with securing the sensor network have more complexity when the group communication of the network is considered. This paper addresses the security issues associated with the Group key management techniques and ensures some significant conclusions for group key management in cluster tree WSNs. A group is defined as a set of sensor nodes present in cluster based tree network and shares some sensory information such as temperature, pressure, etc. The main objective of the paper is to highlights some of the significant issues which are associated with the authentication of the group key data exclusively for the members who have a secure access to the group information. This study contributes an overview of secure an efficient group management mechanisms for cluster tree networks and in between group members. In order to focus on the various issues and limitations a comparative analysis of various key management techniques have been done and evaluated. The schemes are allowed to maintain multiple groups and rekey desperately. This paper focuses on the various group key management issues that outperforms conventional techniques of group key management.

Keywords:

Secure group management, Group communication, Wireless sensor networks (WSNs), Security.

1. INTRODUCTION

In the recent technologies Wireless Sensor Networks (WSNs) becomes more efficient techniques for transmitting energy in limited constrained nodes as well as analyzing data’s, processing data, and sensing capabilities.

These sensor nodes have been adopted for a wide range applications, such as health monitoring system, environmental applications, and home automation system as well as transportation applications. As WSNs basically deployed in security applications, such as Military systems, police department, education department, small and very large scale industries etc. wherever require security becomes extremely important. Because these nodes are exposed to many Varity of malicious attacks. In addition to resource and computing constraints, data security in wireless sensor networks contains many different challenges that are very difficult and it is compared with conventional techniques. WSNs have been attracted from several research issues like security purposes, authentication, key distribution techniques, key management system, data confidentiality, data integrity, broadcast security etc., the problems imposed in WSNs has becomes more challenging issue, when dealing with a group security as well as in network managements systems[1]. In addition to these issues several works have been address the problem in many different transmission data through unsecure medium. In addition to several problems have also addresses; however each of them depends on specific and different grouping concepts.

This paper, focused on secure group communication system in cluster tree WSNs, here a group is called a set of many different sensor nodes and sharing common information in private system. Thus, the important challenges like initiation and distribution of a group key in secure and efficient technique also summarized in this paper.

The main objective of the paper is to highlights some of the significant issues which are associated with the authentication of the group key data exclusively for the members who have a secure access to the group information

This paper focuses on the detailed discussion about the survey of group key management techniques based on logic key tree to increase the efficiency of the wireless sensor network. The paper is prepared and presented as follows. Section II gives an overview of the issues associated with group key management and the section III provides the Theoretical details of the group key management and Algorithms, here the Existing System, Research Gap And The Limitations of the Various Proposed group key management Techniques are described in section V and Performance analysis of the proposed systems are represented by graphs. And the conclusion and the future work is elaborated in the section V

2. ISSUES IN KEY MANAGEMENT TECHNIQUES

A wireless sensor network is a special kind of network which has many limitations as compared to a traditional computer networks. Due to these constraints it is difficult to directly employ the existing security approaches to the area of wireless sensor networks. Therefore, to develop useful security mechanisms while borrowing the ideas from the current security techniques, it is necessary to know and understand these constraints first.

2.1 Very Limited Resources

In wireless sensor network sensor nodes consists very memory space and a limited amount storage Space and the sensor node which is a tiny device consists only very less amount of memory space and storage capacity for the programs. To design a security mechanism which can be effective, it is necessary to reduce the size of code of the security algorithm. For example, one common sensor type (TelosB) has a 16-bit, 8 MHz RISC CPU with only 10KRAM, 48K program memory, and 1024K flash storage [2]. With such a limitation, the software built for the sensor must also be quite small. The total code space of Tiny-OS, the de-facto standard operating system for wireless sensors, is approximately 4K, and the core scheduler occupies only 178 bytes. Therefore, the code size should be minimized for the all security and it should also be small.

Power Limitation Energy now days it is found to be the biggest constraint which imposes some issues in wireless sensor capabilities. It has been assumed that when the sensor nodes are organized in a sensor network, they cannot be easily substituted (high operating cost) or invigorated (high cost of sensors). Therefore, the battery charge which is taken with them to the field must be preserved for extending the life of the individual sensor node and the entire sensor network**.**

2.2 Unreliable Data Transmission

Certainly, unreliable data transmission is another threat to the sensor security mechanisms. The security mechanisms of the network which are completely dependable on a defined protocol, which in turn depends on data or packet Transmission.

Unreliable Transfer normally the packet-based routing of the sensor network is connectionless and thus inherently unreliable. Packets may get damaged due to channel errors or dropped at highly congested nodes. The result is lost or missing packets. Furthermore, the unreliable wireless communication channel also results in damaged packets. Higher channel error rate also forces the software developer to devote resources to error handling. More importantly, if the protocol lacks the appropriate error handling it is possible to lose critical security packets. This may include, for example, a cryptographic key modified Even if the channel is trustworthy, the communication may still be unsafe. This is due to the broadcast nature of the wireless sensor network. If packets meet in the middle of transfer, conflicts will occur and the transfer itself will fail. In a crowded (high density) sensor network, this can be a major problem.

2.3 Unattended Operation

Depends on the functionality of the sensor network nodes, where the nodes may be left unnoticed for long phases of time. These results three main warnings to unattended sensor nodes.

2.4 Vulnerable to Physical Attacks

The sensor may be deployed in an environment open to adversaries, bad weather, and so on. The likelihood that a sensor suffers a physical attack in such an environment is therefore much higher than the typical PCs, which is located in a secure place and mainly faces attacks from a network. Managed various Remote management systems of a sensor network that makes it virtually impossible to sense physical tampering which is termed as through temper proof seals. And physical maintenance issues (e.g., battery replacement). Perhaps the most extreme example of this is a sensor node used for remote reconnaissance missions behind enemy lines. In such a case, the node may not have any physical contact with friendly forces once deployed. No Central Management Point A sensor network should be a distributed network without a central management point. This will increase the vitality of the sensor network. However, if designed incorrectly, it will make the network organization difficult, inefficient, and fragile.

2.5 Security Necessities

A sensor network which is considered as a superior type of network can be useful for sharing some unities where it is applied in a typical computer network, the networking necessities also postures unique requirements of its own which is elaborated in Section 3. Therefore, it can be useful for the important requirements of a wireless sensor network as surrounding with the both typical and network necessities and the unique necessities are suited exclusively to wireless sensor networks.

2.6 Data Confidentiality

Data confidentiality is also considered as a one of the most important issues in the field of network security where these problems are addressed first to minimize various security issues in WSNs. the confidentiality describes to the following:

- A sensor network should not do any leakage of sensing information to its neighbor nodes when it is found to be a military application. The data which presents in the sensor nodes can be highly sensitive and important.
- In many applications nodes which transmit highly subtle data, such as key distribution in that case it is extremely essential to design a secure channel for secure mode of communication in a wireless sensor network.
- Public sensor data, which can be identified where sensor identities the information and public keys, should also be encoded to some extent for protecting the data against traffic analysis attacks.

The standard technique which can be useful for keeping sensitive data secret is to encode the data with a secret key which is only useful in receiver's sides, thus achieving privacy.

2.7 Data Integrity

There are various implemented techniques which can be applicable in confidentiality of sensitive data, an intruder will be unable to access the hidden information. However, this doesn't protect the data properly. The adversary can do the modification of the data, for putting the sensor network into confusion.

For example, some wreckage can be added to various malicious nodes for manipulating the information within a packet. After that the new packet is transmitted to the original receiver. Data loss or damage can be occurred in the absence of a malicious node where there is a harsh communication environment.

2.8 Time Synchronization

Most of the sensor network applications are dependent on some form of the time synchronization. For preserving energy, individual radios of many sensors should be turned off for periods of time. Sometime it is also happened like sensors wish to calculate the end-to-end delay of the transmitted packets as it is transmitted in between two pair wise sensors. A cooperative collection of sensor nodes requires group synchronization to detect the various applications etc. various author proposes various secure synchronization protocols for sender-receiver schemes and group synchronization.

2.9 Authentication

An intruder does not always modify the data packets. It can also modify the whole transmitted packet by adding some additional information. So it is very necessary for the receiver to ensure that the information which is used in any decision making process will always have the correct source node. Authentication s very much essential for many administrative tasks such as network programming, controlling sensor node duty cycle. On the other hand it can be said that message authentication is very much crucial for many application in the sensor network. Information authentication gives functionality to the receiver for verifying the data which is sent by the authenticated user or not. A purely symmetric technique can be applied if the data communication is a two party communication. In this type of mechanism sender and receiver uses a shared secret key for encoding and decoding the data respectively. In the concept of TESLA system a sender will broadcast a message with an auto generated key. And after a period of time the sender reveal the secret key also in the network. The receiver's functionality is to buffering the packets till the secret key is disclosed.

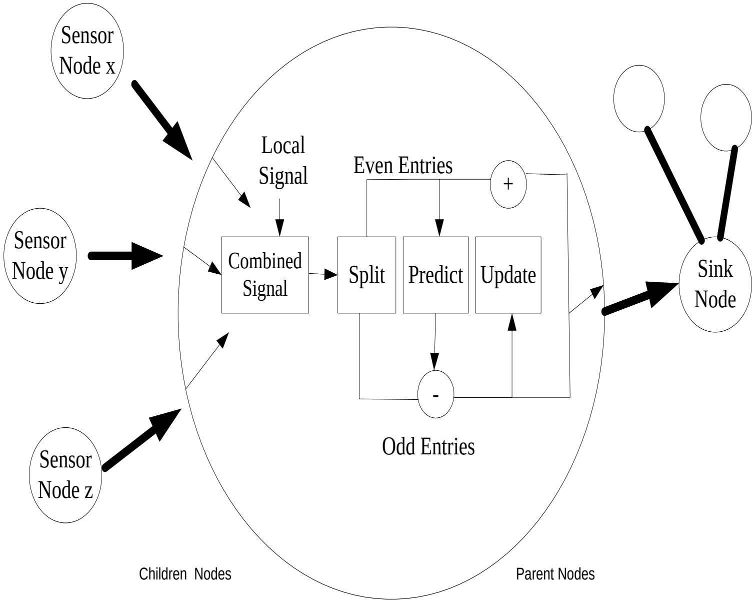

Fig.1. Security of group key management schemes (*Image Source*: Google Image)

3. GROUP KEY MANAGEMENTS IN WIRELESS SENSOR NETWORKS (WSNS)

Different sensor nodes in a wireless sensor network (WSN) collect data from their surrounding and report it to the centralized sink node. The sensing or reporting action of the sensor nodes are regulated by the control signal broadcasted from the centralized sink node. Typical WSNs use multicast tree topologies rooted from sink due to the many-to-1 or 1-to-many communication characteristics. For designing a communication protocol for this topology we need to consider the energy efficiency as it is a major design criteria due to the energy limitation of the sensor node. This is also applicable for designing WSNs security services. In addition of security performance the security service should also consider the energy efficiency of its protocol.

The confidentiality of message is very crucial security primitive for different security service in a sensor network. In general for message confidentiality a network-wide group key (GK) is used for encryption or decryption of the message. In order to prevent a comprised node from decrypting the sink needs to update the GK occasionally. A simple solution is separately distributing new GK for every node after encrypting it with each nodes respective individual key that is shared in between the individual node and the sink. However, rekeying message (N) will be generated with a network size N.

Number of rekeying message is reduced to O (long N) by logical key hierarchical (LKH) by building a tree of key encryption key (KEKs).On the basis of LKH many researchers have further tried to reduce the number of rekeying message with a trade-off local key computation. In these methods depending upon the logical position in logical tree each node will require several keying message out of many keying messages .incase of multi-hop WSN in which each node routes data belong to other node, rekeying generated from the logical key needs to be forwarded to various irrelevant node before arriving at its destination. In other words, the logical tree based method suffer from large communication overhead in a multi-hop WSN surrounding as the key tree structure does not demonstrates the fundamental network topology.

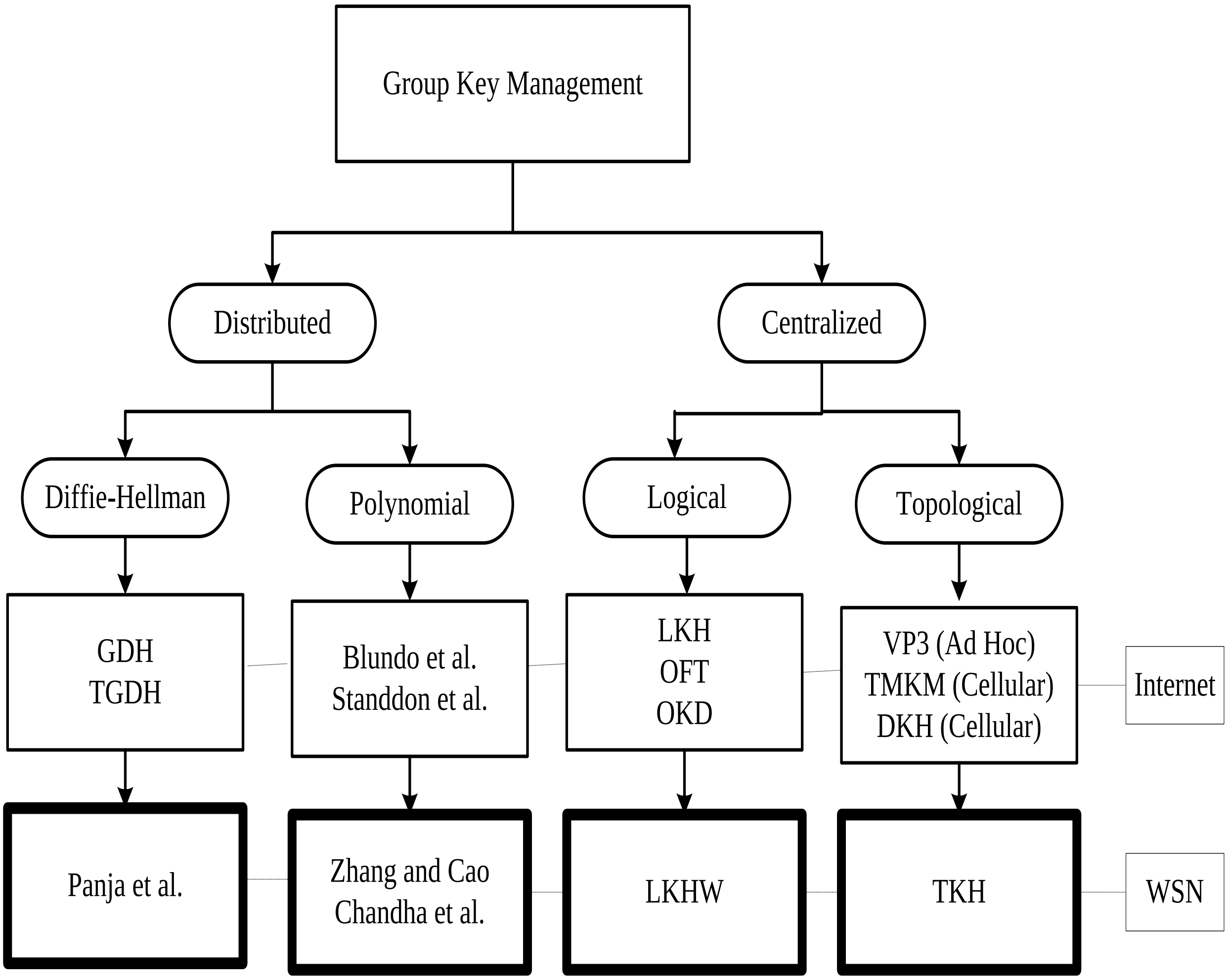

Fig.2. Taxonomy of group key management schemes [3]

4. RELATED WORK

Younis et al [4] designed an auto-management technique to increase the network lifetime as wireless sensor nodes operates on batteries and have a limited amount of energy. The result analysis shows the effectiveness of the behavioral model. The performance analysis shows alkaline batteries have an estimate error inferior to 2%.

Yu et al [5] proposed a constrained random perturbation based pairwise key establishment scheme to mitigate the various security issues of WSN. The performance analysis shows the effectiveness of the proposed system which is practically implemented on the TelosB compatible mode for evaluating corresponding performance and overhead.

Alagheband et al [6] presented the functionality of a key management framework which is based on elliptical curve cryptography technique. The performance analysis shows that the proposed framework individually gives the better secure efficient communication. The proposed technique is considered to be better in terms of communication, computation, and key storage.

Barachi et al [7] proposed a presence based architecture for wireless sensor network / IMS integration. Where the proposed architecture rely on two key components which are a WSN/IMS gateway acting as an interworking and the other one is an extended presence server which is responsible for serving as a context information managing. The performance analysis of the proposed Scheme has been evaluated using some framework.

Kantarci et al [8] evaluated the performance of an in home energy management (iHEM) application where the objective of the proposed system is to mitigate the energy expenses of the consumers. The performance analysis of the proposed system shows the proposed architecture reduces the expenses of the consumers for each case.

Perrig et al. [9] designed a key-chain distribution system for their μTESLA secure broadcast technique where the concept of the μ-TESLA system is to achieve asymmetric cryptography by delaying the disclosure of the symmetric keys. The concept of proposed technique highlights that a sender will transmit a message generated with a secret key. After a certain period of time, the sender will disclose the secret key.

Cunha et al [10] presented an energy efficient battery remaining capacity estimation technique where the important issues are research of the state of charge (SoC), the comparative analysis shows the effectiveness of the proposed system. The experiments have been performed with the use of MICA2 wireless node platform. The performance outcomes show voltage only based estimation presented an available 18% of the battery and the maximum capacity.

Ren et al [11] proposed allocation aware end to end security framework to mitigate the various security issues associated with the wireless sensor network. The performance analysis of the proposed system assures both node to sink and node to node authentication. Comparative analysis shows that an efficient bogus data filtering technique works properly and the proposed system is highly re salient against the various DoS attacks.

5. RESEARCH ISSUES

Although in the past research efforts have been introduced on cryptography, key organization, safe routing, protected data aggregation, and intrusion detection in WSNs, there are still some challenges to be addressed. First, the selection of the appropriate cryptographic methods depends on the processing capability of the sensor nodes, indicating that there is no unified solution for all sensor networks. Instead, the security mechanisms are highly application specific. Second, sensors are characterized by the constraints on energy, computation capability, memory, and communication bandwidth. The design of security services in WSNs must satisfy these constraints. Third, most of the current protocols assume that the sensor nodes and the base stations are stationary. However, there may be situations, such as battlefield environments, where the base station and possibly the sensors need to be mobile. The mobility which is a characteristic of the sensor nodes has a great impact on sensor network topology and thus raises many issues in secure routing protocols. Some future trends in WSN security research are identified as follows: Exploit the availability of private key operations on sensor nodes: recent studies on public key cryptography have shown that public key operations are still very expensive to realize in sensor nodes. A public key cryptography technique can be used for the comfortable design of security techniques in the area of WSNs which improves the efficiency in various private key operations of sensor nodes which are highly desirable for secure routing. Various secure routing protocols of mobile sense networks have been designed and has a great impact of sensor network topology and the in the field of routing protocols the mobility factor can be used at the base station, sensor nodes, or both. Current protocols assume the sensor network is stationary. New secure routing protocols for mobile sensor networks need to be developed. Time synchronization issues: current broadcast authentication schemes such as μ-TESLA and its extensions require the sensor network to be loosely time synchronized. This requirement is often hard to meet and new techniques that do not have such requirement are in demand. Scalability and efficiency in broadcast authentication protocols: new schemes with higher scalability and efficiency need to be developed for authenticated broadcast protocols. The recent progress on public key cryptography may facilitate the design of authenticated broadcast protocols. QoS and security: performance is generally degraded with the addition of security services.

Table.1. Existing Techniques

Authors	Problems Identified	Techniques Applied	Performance Parameters
Yetgin et al. [12]	High Energy Consumption In Wireless Sensor Network	Signal Processing Power (SSP) P_{SP} On Network Lifetime.	Signal To Noise Ratio Bit Error Rate Periodic Transmit Time Slot
Qian et al. [13]	Security And The Survivability Of Wireless Sensor Network.	Security And Survivability Architecture	Signal To Noise Ratio Bit Error Rate Periodic Transmit Time Slot
Yang et al. [14]	Low Resource , Highly Dynamic , And Vulnerable Sensor Networks	Autosp-WSN A Novel Framework	Reliability Sustainable Operation Network Utility
Wang et al. [15]	Challenges Related To The Integration Of WSN.	A Five Layer System Architecture	Synergistic Performance
Bechkit et al. [16]	Sensitivity Of The Potential WSN	Unital Design Theory	Storage Overhead Network Scalability
Ruj et al. [17]	Triple Key Establishment Problems In Wireless Sensor Networks.	A Polynomial-Based And A Combinatorial Approach	Pairwise And Triple Key Distribution
Ma et al. [18]	Energy Consumption Issues And Reliable Communication	Contiguous Link Scheduling Problem	Storage Overhead Network Scalability
Gu et al. [19]	Issue Of End To End Secure Communications	Differentiated Key Pre-Distribution	Pairwise And Triple Key Distribution
Seo et al. [20]	Securing Data And Communications	CL-EKM In Contiki OS	Time Energy Memory Performance Communication

Klaoudatau et al. [21]	Complexity Of Various Protocols In WSN	Cluster-Based Group Key Agreement	Complexity Of Each Protocol And The Energy Cost
Yu et al. [22]	Harsh Environments	Fault Detection, Diagnosis, And Recovery	Storage Overhead Network Scalability
Dong et al. [23]	Challenges In The OS Design Space	Discuss Evaluations Of A Sensornet OS	Reliability Sustainable Operation Network Utility
Li et al. [24]	Dependability Of A Trust System	Lightweight And Dependable Trust System (LDTS)	Communication Overhead Memory Performance
Ruiz et al. [25]	Absence Of Management Solution In WSN.	MANNA Architecture	Storage Overhead Network Scalability
Camtepe et al. [26]	Secure Communication In WSN	Novel Deterministic And Hybrid Approaches Based On Combinatorial Design	Connectivity With Smaller Key-Chain Sizes
Poornima et al. [27]	Energy Consumption Issues	Mobile Data Collector (MDC)	Energy Consumption Secure Data Collection

6. CONCLUSION

A mutual healing key distribution method by using bilinear pairing is suggested in this paper. Security module mutual healing key distribution formal definition was discussed. The suggested scheme accomplishes many desirable features. Each node's storage overhead is a constant. The method is free of any coalition for illegitimate nodes. Private key of each authorized node has nothing to do with that of, number of nodes revoked and if it is not disclosed it can be reused. Based on the secret sharing self-healing key distribution method, the reusing of personal key can be done on the condition if less than the amount of threshold nodes is revoked. In addition their method allows recovering of the node from single broadcasting message that is associated with all keys in the session to the session group to which they belong. The suggested mutual-healing method relies on identification and location based keys. These indicate that the suggested method can be used only over wireless networks where nodes will be stable. Realizing mutual-healing in mobile wireless networks is not a trivial issues. Mutual-healing method is largely useful in mobile wireless networks because of lower connectivity of network of mobile wireless network than a steady wireless networks. Therefore it is important to investigate new schemes to realize the mutual-healing attribute mobile wireless network.

7. REFERENCES

[1] Ameen, A., and Kwak, K. S.2011. Social Issues in wireless sensor networks with healthcare perspective. Int. Arab J. Inf. Techno, Vol. 8(1), pp. 52-58

[2] Sen, J.2012. Security in wireless sensor networks. Wireless Sensor Networks: Current Status and Future Trends, Khan, pp. 407-460

[3] J-H.S and S-W.S.2015.Group Key Managements in Wireless Sensor Networks. www.intechopen.com

[4] Younis, M., Ghumman, K., Eltoweissy, M.2006. Location-Aware Combinatorial Key Management Scheme for Clustered Sensor Networks. Parallel and Distributed Systems, IEEE Transactions, Vol.17, No.8, pp.865-882

[5] Yu, M., Mokhtar, H., Merabti, M .2007. Fault management in wireless sensor networks. Wireless Communications, IEEE, Vol.14, No.6, pp.13-19

[6] Alagheband, M.R., Aref, M.R.2012. Dynamic and secure key management model for hierarchical heterogeneous sensor networks. Information Security, IET, Vol.6, No.4, pp.271-280

[7] Barachi, M., Kadiwal, A., Glitho, R., Khendek, F., Dssouli, R.2010. The design and implementation of architectural components for the integration of the IP multimedia subsystem and wireless sensor networks. Communications Magazine, IEEE, Vol.48, No.4, pp.42-50

[8] Erol-Kantarci, M., Mouftah, H.T.2011.Wireless Sensor Networks for Cost-Efficient Residential Energy Management in the Smart Grid. Smart Grid, IEEE Transactions, Vol.2, No.2, pp.314-325

[9] Anderson, R., Haowen, C., Perrig, A.2004. Key Infection: Smart Trust for Smart Dust, 20 in: 12th IEEE International Conference on Network Protocols (ICNP), Berlin, Germany, 206–215

[10] da Cunha, A.B., da Silva, D.C.2012.Behavioral Model of Alkaline Batteries for Wireless Sensor Networks. Latin America Transactions, IEEE (Revista IEEE America Latina), Vol.10, No.1, pp.1295-1304

[11] Ren, K., Lou, W., Zhang, Y.2008. LEDS: Providing Location-Aware End-to-End Data Security in Wireless Sensor Networks. Mobile Computing, IEEE Transactions, Vol.7, No.5, pp.585-598

[12] Yetgin, H., Cheung, K.T.K., El-Hajjar, M., Hanzo, L.2014. Cross-layer network lifetime optimization considering transmit and signal processing power wireless sensor networks. Wireless Sensor Systems, IET , Vol.4, No.4, pp.176-182

[13] Qian, Y., Lu, K., Tipper, D.2007. A design for secure and survivable wireless sensor networks. Wireless Communications, IEEE , Vol.14, No.5, pp.30-37

[14] Yang, S., Yang, X., McCann, J.A., Zhang; T., Liu, G., Liu, Z.2013. Distributed Networking in Autonomic Solar Powered Wireless Sensor Networks. Selected Areas in Communications, IEEE Journal, Vol.31, No.12, pp.750-761

[15] Wang; L., Xu, L.D., Bi, Z., Xu, Y.2014. Data Cleaning for RFID and WSN Integration. Industrial Informatics, IEEE Transactions, Vol.10, No.1, pp.408-418

[16] Bechkit, W., Challal, Y., Bouabdallah, A., Tarokh, V.2013. A Highly Scalable Key Pre-Distribution Scheme for Wireless Sensor Networks. Wireless Communications, IEEE Transactions, Vol.12, No.2, pp.948-959

[17] Ruj, S., Nayak, A., Stojmenovic, I.2013. Pairwise and Triple Key Distribution in Wireless Sensor Networks with Applications. Computers, IEEE Transactions, Vol.62, No.11, pp.2224-2237

[18] Ma, U., Lou, W., Li, X-Y.2014.Contiguous Link Scheduling for Data Aggregation in Wireless Sensor Networks. Parallel and Distributed Systems, IEEE Transactions, Vol.25, No.7, pp.1691-1701

[19] Gu, W., Dutta, N., Chellappan, S., Bai, X.2011. Providing End-to-End Secure Communications in Wireless Sensor Networks, Network and Service Management, IEEE Transactions, Vol.8, No.3, pp.205-218

[20] Seo, S-H., Won, J., Sultana, S., Bertino, E.2015. Effective Key Management in Dynamic Wireless Sensor Networks. Information Forensics and Security, IEEE Transactions, Vol.10, No.2, pp.371-383

[21] Klaoudatou, E., Konstantinou, E., Kambourakis, G., Gritzalis, S.2011. A Survey on Cluster-Based Group Key Agreement Protocols for WSNs. Communications Surveys & Tutorials, IEEE, Vol.13, No.3, pp.429-442

[22] Yu, C-M., Lu, C-S., Kuo, S-Y.2010. Noninteractive Pairwise Key Establishment for Sensor Networks. Information Forensics and Security, IEEE Transactions, Vol.5, No.3, pp.556-569

[23] Dong; W., Chen, C., Liu, X., Bu, J.2010. Providing OS Support for Wireless Sensor Networks: Challenges and Approaches. Communications Surveys & Tutorials, IEEE , Vol.12, No.4, pp.519-530

[24] Wang; L., Xu, L.D., Bi, Z., Xu, Y.2014. Data Cleaning for RFID and WSN Integration. Industrial Informatics, IEEE Transactions , Vol.10, No.1, pp.408-418

[25] Ruiz, L.B., Nogueira, J.M., Loureiro, A.A.F.2003. MANNA: a management architecture for wireless sensor networks. Communications Magazine, IEEE , Vol.41, No.2, pp.116-125

[26] Camtepe, S.A., Yener, B.2007. Combinatorial Design of Key Distribution Mechanisms for Wireless Sensor Networks. Networking, IEEE/ACM Transactions, Vol.15, No.2, pp.346-358

[27] Poornima, A.S., Amberker, B.B.2011. Secure data collection using mobile data collector in clustered wireless sensor networks. Wireless Sensor Systems, IET , Vol.1, No.2, pp.85-95