International Journal of Advances in Applied Sciences (IJAAS)
Vol. 6, No.1, March 2017, pp. 22~30
ISSN: 2252-8814

MTKD: An algorithm for Multi-Tier Key Distribution for securing Group Communication in WSN

Annapurna H S[1], M. Siddappa[2]
[1]Dept of CSE, SSAHE, Tumkur, India
[2]Departement of CSE, SSIT, Tumkur, India

Article Info

Article history:

Received Jan 8, 2016
Revised Feb 11, 2017
Accepted Feb 19, 2017

Keyword:

Group Communication
Key Management
Pairwise Key Distribution
Wireless Sensor Network

ABSTRACT

Security is one of the inherent challenges in the area of wireless sensor network. At present, majoroty of the security algorithm are incorporated with massive iterations of cryptography as well as complex mathematical modelling that result in degradation of quality of service. The present paper takes the case study of group communication in wireless sensor network and introduces a significant protocol that assist in generation of joint key with an aid of unique and lightweight cryptography. The outcome of the study was compared with the most significant and standard work of group communication to find that proposed system is in adherence of time and space complexity.

Corresponding Author:

H.S Annapurna,
department of Computer Science & Engginering
Sri Siddhartha Academy of Higher Education, Tumkur, India.

1. INTRODUCTION

Wireless sensor network(WSN) , concerned the awareness of the explore sections other then two decades owing to its probable benefit in observe the remote data and inherent issues in the procedure. The data that flows in among the sensor nodes in wireless sensor network consist of physically captured data from the readings of sensors, a mobile code, security using key management techniques, and location information of the sensor nodes. Owing to the lesser amount of obtainable of computational origin in the miniature sensor nodes and wireless communication socail, wsn endure from probable security threat aspect [1]. There are basically two types of attacks in sensor network e.g. active and passive attacks [2]. The malicious nodes can enhance their attacking capabilities by intruding the private information from mobile codes as well as by accessing the information pertaining to the positioning of the nodes [3]. Using various eavesdropping technique, it is possible for the malicious node to incorporate a malicious programmes on the mobile code and thereby spreading the malicious mobile code in the entire network. The malicious node can also use the position information to identify the best node to invoke their attacks thereby potentially making security breach. Owing to the wireless medium of communication in wireless sensor network, it is very challenging task to identify the malicious nodes and design a security policy to deny the access in the network. The malicious nodes are quite capable enough to access the entire network using potential computers and sophisticated communication equipments. The malicious nodes can also seed themselves in the network environment without even getting caught [4]. It is said that sink is considered as the most reliable core of the wireless sensor network that stores significant information about the security protocols, readings of sensors, and routing information. These are very critical in group communication. In small scale sensor network, it is easier to capture the data, process it, and forward to sink. But in random and dynamic network of large size, it usually don't go by single hop communication. The nodes are formulated in groups, where each group member interacts with other group member to forward the processed data from one to another point. The

process of data aggregation completely fails without group communication. Hence, it is very important that a robust security technique to be developed to address the security issues in group communication system in wireless sensor network. Cryptography [5] is the most frequently adopted technique to incorporate security while performing group communication in wireless sensor network.

However, conventional cryptographic algorithms like SHA, AES, although have good security features, but they suffers from limitations too. Adopting a cryptographic technique also have various limitations too e.g. i) it can ensure an effective key management, but cannot jointly ensure the communication performance of the large scale network, especially the time critical applications in wireless sensor network, ii) cryptographic protocols works in recursive manner with various iterative and complex steps of encryptions and thereby they gives rise to both time and space complexity, while working on secure group key management techniques, iii) adoption of cryptographic technique emphasize much on key generation but not much on ensure a second layer of protection of the generated key in case of different adversarial activities, iv) the conventional mechanism of broadcasting of the encrypted keys (as a mobile code) can be overhear by the malicious node. Hence, keeping all these issues in mind, the present paper introduces a technique of secure group key communication. Section 2 discusses about the prior research work followed by brief discussion of problem identification in Section 3. Section 4 discusses about the proposed system followed by illustrated description of design principles in Section 5. Algorithm implementation is discussed in Section 6 followed by result discussion in Section 7. Section 8 summarizes the paper.

2. RELATED WORK

The study towards secure group communication is more than a decade old and there are various techniques that have been introduced by the various researchers. This section discusses some of the recent studies found in standard research manuscript that focuses on i) secure group communication and ii) key distribution mechanism.

Cheikhrouhou et al. [6] have introduced a protocol for ensuring secure group communication over ring based topology of wireless sensor network. The authors have discussed their outcomes considering storage cost which was found to be efficient compared to existing technique. However, the limitation of the study is the dependency of key storage of size 160 bits using elliptical curve cryptography. Bechkit et al. [7] have introduced a pre-distribution of keys for ensuring network scalability. The advantage of the protocol was its equal key ring size and limitation of the scheme was non-volatile nature of the session key sharing which is not actually resilient against many lethal attacks in wireless sensor networks. Khalid et al. [8] has jointly used combinatorial and traversal design principle for performing secure distribution of keys. The study also bears the limitation of higher dependency of secret key which is not secured. Moreover the system is only resilient against node capture attack and not for other types of attacks. Mi et al. [9] have emphasized on positioning of the secret keys while perform distribution using Global Positioning System, which is an expensive process of incorporating security. Oliveira et al. [10] have proposed a technique of pairing based encryption on real-time motes. Although the key size in 386 bits in RAM, there is a further probability of minimizing the size. Such key-size is not compatible for higher iterations or for large scale wireless sensor network. Sanchez et al. [11] have proposed a security protocol for wireless body area network. Although the scheme enables flexibility in decryption operation, the security of the generated key is not much emphasized. Moreover, the process suffers from recursive rounds of encryption. Bellazreg and Boudriga [12] have presented a key management technique to ensure secure group key structure as well as to address need of dynamic tunneling. The advantage of this scheme is regular updates of keys and the limitation of the scheme is it supports only one-tunnel per group for enabling communication. The scheme also doesn't explicitly discuss about the time and storage complexity. Morchon et al. [13] have proposed a cost-effective predistribution of keys that provides identity-based security in wireless sensor network. One advantage of the scheme is it is independent of any interaction process to generate or authenticate keys. However, the outcome was tested with very less size of data and may not be applicable in multi-hop communication of keys. Wang et al. [14] have proposed a predistribution policy considering hexagonal grids consisting of groups and keys. Miettinen et al. [15] have presented a security protocol by incorporating an authenticated pairing system based on key context. Furtak and Chudzikiewicz [16] have used asymmetric key pair as well as electronic signature to provide secure authentication in wireless sensor network. Xi et al. [17] have presented a key estimating process that is done in faster manner as compared to attacker. However, various attacker have various patterns of generating attacks, the authors have not discrete mentioned the names of the attack. Moreover the outcomes of the study were not found to be benchmarked.

Hence, it can be seen that there exist various security protocols in the research papers with advantages and limitations. The prime trade-off found in all the study is dependency of broadcasting the key. We comment that broadcasting of the key is very sensitive operation and is highly prone to capture if proper

encryption scheme is not implemented. Another trade-off found is majority of the scheme is based on enhancement of conventional cryptographic scheme with less novelty in mathematical approaches. The third trade-off seen in all the studies are about the key sizes, which is 128, 216, 160, or 512 bits. Although the key sizes seems to be smaller but as majority of the existing approaches stores this, grossly the sizes of the matrix holding the keys becomes eventually larger.

3. PROBLEM IDENTIFICATION

The suggest system is mostly the matter connected with conservative key management method appropriate in WSN. For an effective key management method, the structure should make certain exponentially superior level of resiliency, conflict, and revocation. The brief discussions on the identified problems are:

a. Work toward prevention system is more important compared to work towards detection system. Whatever is the pattern of attack, usually the attacker compromise a node and it either perform a replica of compromised node or it itself participate in data dissemination process. The nodes are usually represented by node ID, for which reason, it becomes difficult for the other node to understand the origination point of attack.
b. The adversary can also generate colluding attacks. Hence, when the sensor nodes execute distribution of their keys, their negotiation near nodes (if any) ultimately comes concerning the key-information.
c. A node in a network is concession that it escorts to susceptibility effect other nodes too. The compromised sensor node should not disclose any private information of the other nodes.
d. Superiority of the presented system is flexibility towards precise form of attacks. Hence, when the attack scenario changes, the solution to thwart the attack is no longer applicable. Hence, there is a need of a system that introduces a technique for circumventing majority of the lethal attacks towards key management schemes in wireless sensor network.

4. MULTI-TIER KEY DISTRIBUTION IN WSN

The model is coined as MTKD i.e. Multi-Tier Key distribution mechanism that is mainly designed to incorporate higher level of security mechanism in key management during data aggregation in wireless sensor network as well as to perform group communication.

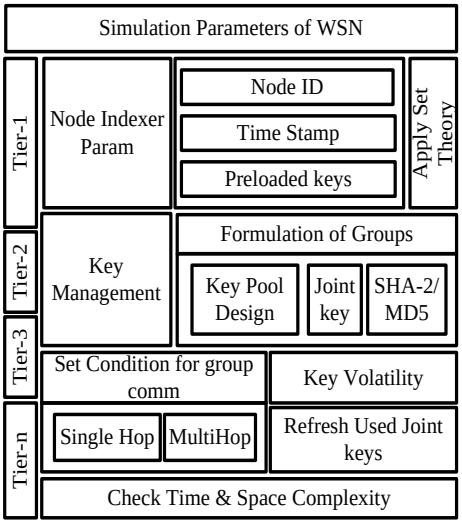

Figure 1. Proposed MTKD Schema

Figure.1 highlights the schema of the proposed system considering various ranges of attacks e.g. Node Capture Attack, Denial-Of-Service, Tunneling Attack, Sybil attack. Supported by empirical and mathematical modelling, the proposed system ensures complete security of group communication for large scale wireless sensor network. The elaborated discussion of Figure 1 and its mathematical strategies is done with respect to design principles in next section.

5. DESIGN PRINCIPLE OF MTKD

The design of the proposed MTKD model is completely based on the novel mathematical approach that initiates by considering two-dimensional matrix of single-tier of architecture designs (KP, SN), where KP is the set of key indexers, while SN is the mote that consist of specific key indexer from KP. The indexers will consists of mainly three information i.e. node ID, time stamp, preloaded key. The process of key-allocation and giving a mathematical shape is not easy as it is quite possible that every sensor nodes have different number of keys. Hence, to ease off the computation, MTKD considers equal number of key distribution in every sensor nodes. It applies set theory to map the key pools and its associated relationship with secure key-managements.

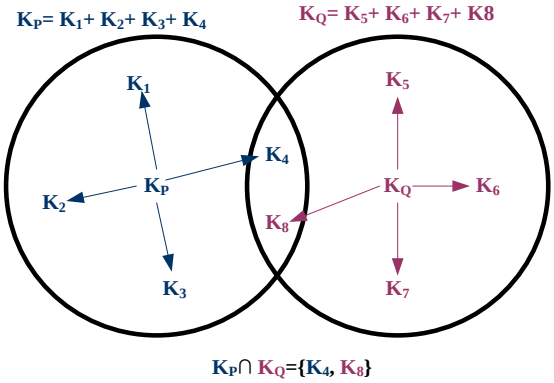

Figure 2. Set Theoretical Representation of Key Pools

The above Figure2 shows the condition of the key-distribution scheme in MTKD as well as finding the joint-key to enable secured group communication. It shows that two key-pools KP {=K1+K2+K3+K4} and KQ {=K5+K6+K7+K8} for PTH group and Qth group in wireless sensor network, which has their own individual keys. The system formulates a condition of KP∩KQ to extract the joint key that is required to perform group communication. Hence, the formulation of joint key is KJ= KP∩KQ. The condition states that any sensor node of PTH group will be able to perform communication with other sensor node of Qth group will require to have Kj (such that KJ≠0). In this process, the sensor nodes will broadcast only their indexers. Based on the modelling, MKTD designs an algorithm, which is very simple and yet unique, to be running in a sensor mote. The system will enable the one node in PTH group to estimate joint key KJ with other node in Qth group. In this example, the joint key is K4 and K8, which is again subjected to encryption along with the indexers of two nodes σP and σQ. One interesting fact of security is that as K4 and K8 are unique, hence performing concatenation of them will also yield a unique value. The mechanisms will also the adjacent nodes in proximity of transmitting nodes to evaluate the common indexers between node in PTH group and node in Qth group as well as indexers of their joint key too. The advantage of this mathematical modelling is that as the adjacent node cannot posses both the key information (K4 and K8) so it is near to impossible to guess the concatenated values of both the keys (K4 and K8). This principle ensures that even a legitimate member, who is not the transmitting (or clusterhead) node can posses the joint key KJ at any instance of time. However, there is another vulnerable situation especially in case of node capture attack, which completely compromise the sensor node and its resources. In such attack scenario, it is quite possible that the compromised member node may perform colluding attacks and extract the values of K4 and K8. In order to resist such event, the proposed system will incorporate volatility of all the joint keys, which means in this case, one K4 and K8 are evaluated as joint key and the node uses it to perform communication. Once the communication is over, K4 and K8 is refreshed to generate new key values unknown to the attacker. Sensor network performs communication of data using various routing principles, which are described in terms of Tiers of architecture:

a. **Tier-1**: A member node captures the data and forwards the data to clusterhead. It has to ensure that it is actually forwarding the data to the clusterhead and not any rogue nodes (in case of eavesdropping or tunneling attack). Hence, the proposed principle ensure two facts i.e. i) owing to one indexers as time-stamp, the data redundancy can be addressed in the primary level of data dissemination process, and ii) all the member nodes should evaluate joint keys for clusterhead in sequential manner. Hence, security with data redundancy is addressed in Tier-1 of architecture.

b. **Tier-2**: After the data is gathered from the member nodes, the clusterhead must find a way to forward the data to the sink. As there are various routing algorithms existing [18][19][20] that is compatible with single-hop (directly to sink) and multi-hop (via other clusterheads to sink), so present technique performs multi-layered authentication technique to encrypt their data. For single hop network, the joint key is encrypted just one time, however, for multi-hop network, the encryption of the joint-key is done based on the number of hops, it requires the data to travel. Hence, the proposed system ensures security over each unit link of communications.
c. **Tier-3**: After the accomplishment of communication, it is essential that used joint keys are **simultaneously** refreshed to resist the possibility of using stale keys. The proposed system doesn't wait for complete communication to happen from source to destination, rather, it makes the joint key volatile in every single link utilization in the communication process. Hence, it significantly reduces the overhead as well doesn't yield significant storage complexity.
d. **Tier-n**: At present there are various techniques of reconfigurable architecture, where the wireless sensor network is integrated with optical network [21] or cloud environment [22] or any other networking technologies. The proposed system supports equal level of security by ensuring that only the communication nodes do have access on joint keys. This principle is highly resilient against maximum attacks on security keys.

6. ALGORITHM IMPLEMENTATION

The proposed system is designed using Matlab. The implementation of the MKTD is done considering 500 sensor nodes on 1200x1000 m2 simulation area. The preliminary phase of the simulation is carried out by considering assigning set of indexers randomly to all the sensor nodes present in the network. The system also provides a key along with these indexers. The communication only initiates of two nodes from different groups are found with joint keys. The proposed system offers security on every tier of proposed architecture. For this purpose the system initially considers assuming attacker module that has recently intruded the network either using inside or outside attacking strategy. Existing techniques usually is experimented using 128 or 512 bit of encryption keys. However, the proposed system offers highest level of flexibility by offering differential the key size. This is the most unique features of MKTD design principle. Because of this principle, MKTD offers security in every tiers of proposed architecture.

Depending on the type of application to be used, the proposed system also offers higher flexibility to use any deployment strategies for sensor nodes. However, the experiments have been carried out and outcomes were analyzed mainly with an aid of random deployment strategies. A node belonging to PTH group can only establish secure communication with node in Qth group, if they have joint key. The designs of the joint key plays a critical role and therefore, they were incorporated with following features e.g.

a. Owing to differential key size, the storage cost is minimized that is directly equivalent to the set of the secret keys being stored in matrix,
b. Increases probability of two groups to perform communication as it supports both single and multi-hop communication technique
c. Reduced spatial distance between the two communication nodes either in same or in different groups
d. Owing to volatile nature of the keys and encryption technique, the keys are highly secured in case of any attacks in wireless sensor networks
e. Due to frequent updates of keys after the expiry of the old joint keys, it leads to significantly less overhead for the purpose of generating new joint keys. Hence, memory size is totally independent of number of communication being taking place.

An interesting point to observe in the proposed algorithm design is that joint keys are accessible to only communicating nodes strictly. Even neighbor nodes don't have accessibility. Hence, in case of any routing attacks or node compromization attacks that intrudes any member nodes doesn't have any impact on secure group communication in the present scenario. In many existing system [23][24][25], it was found that sensor nodes broadcast key information to other nodes; however, there is a possibility that an attacker can posses this key information during broadcasting process of the source node. However, MKTD scheme doesn't broadcast any key indexers for the purpose of extracting joint keys, hence; it is completely resilient against maximum possible threats.

The algorithm designed against the proposed mathematical model can be represented as:

Algorithm: Multi-Tier Key Distribution in WSN
Input: WSN Node parameters

Output: Generation of Joint Key
START
1. Initialize the size of key (k) (~128 bit)
2. Initialize the indexer of *i* and *j* node
   Id_i=[x, y, z] Id_j=[x_1,y_1, z_1];
3. **IF** (z= =z_1)
4. **Return** 'No Joint Key';
5. Return NULL;
6. **ELSE**
7. g=abs((x-x_1)^2+4(y-y_1));
8. **IF** (sqrt(g) ~=0)

$$K_{j1} = \frac{(x-x_1) \pm \sqrt{(x-x_1)^2 + 4(y-y_1)}}{2} |z|$$

K_{J1}=K_{J1}+1;
K_{J1}=round(K_{J1});

$$K_{j2} = \frac{(x-x_1) \pm \sqrt{(x-x_1)^2 + 4(y-y_1)}}{2} |z|$$

K_{J2}=K_{J2}+1
K_{J2}=round(K_{J2});
9. **IF** (K_{J1}<k , K_{J2}<k)
10. X_{ij}= concat (K_{J1}, K_{J2})
11. X_{ij}=maximum (X_{ij});
12. Data=concat (X_{ij}, Id_i, Id_j);
13. Generate Joint Key
14. K_J=Encrypt (Data, 'SHA2/MD5');
15. **Return** K_J;
16. Use K_J in communication
17. **ELSE**
18. Return 'No Joint Key'
19. **END IF**
20. **ELSE**
21. Return 'No Joint Key'
22. **END IF**
23. **END IF**
END

The proposed algorithm considers i node to posses (x, y, z) indexer that intends to perform communication with j node with (x1, y1, z1) indexers. The first component of the indexers (x, x1) specifies node identity, the second component of the indexers specifies time stamp (y, y1), and third component of the indexers specifies key (z, z1). Hence, when z is found equivalent to z1, than node i and j are said to be in condition for not generating the joint keys. This possibility is set as it is possible that certain attackers attempts to intrude the network and steal the key information either z or z1. In such cases, the intruders will posses either z or z1 and not the both. Hence if either z or z1 is compromised and replica key is broadcasted in the network, than MTKD must ensure to identify such replicated keys and must break the communication if it is found. Hence, the algorithm has the capability to identify the key replicas introduced by malicious node. In case of the situation when z≠z1, than a joint key is extracted using

$$K_j = \frac{(x-x_1) \pm \sqrt{(x-x_1)^2 + 4(y-y_1)}}{2} |z| \quad (1)$$

Hence, if the second component of eq.(1) exists than it is possible to extract two joint keys KJ1 and KJ2 (just like K4 and K8 in the example). The system performs concatenation of both the extracted keys and

performs encryption by additionally concatenating with indexers of i and j node. As the proposed system is designed to address the security issues in multi-tier architecture of group communication in wireless sensor network, so the values to be assigned for x, y, and z for i node remains constant, while the value of x1, y1, and z1 are altered based on number of tiers to be addressed. There is also a possibility that the intruder might know the scheme of generating the joint keys, but until and unless it don't have keys (like z and z1), it will never be able to extract the encrypted joint keys.

7. RESULT ANALYSIS

For the purpose of performing comparative result analysis, the proposed system considers the work done by Zhang et al. [26] who has introduced a technique for pairwise key establishment policy in sensor networks. The prime highlights of methodology used in Zhang et al. [26] work are e.g. i) used mesh structure to store the seed of key, ii) neighbor sensor can extract the pairwise key information for accomplishing group communication, iii) the key establishment is carried out by system authority, routers, and sensor nodes, iv) Used AES algorithm of 128 bit for ciphering the key. The outcome of the work being carried out by Zhang et al. [26] is evaluated using storage cost mainly. Hence, although the motive of Zhang et al. [26] is same like us, but they differ in their approach. In order to carry out comparative analysis, the core algorithm of Zhang et al. [26] was experiment in similar platform to testify the outcomes.

Figure 3 showcases the outcome accomplished by the proposed MTKD with Zhang et al. [26] study with respect to processing time. The outcome shows that Zhang et al. [26] approach significantly takes more processing time with the increase of iteration, where each iteration will signify increasing data dissemination process. The data packet was tested with 500-15000 bytes of data in increasing order to check how long the system takes to process the core algorithm. Zhang et al. [26] approach although is more resilient against node capture attack, but looking into the incrementing pattern of the curve, it cannot be said to be robust against Denial-of-Service attack. Although authors have discussed a robust accomplishment of computational complexity in their research paper, but when the attacker module is changed, the outcome shows to no enhancement in processing time. Proposed MKTD uses a novel approach where cryptographic encryption is extremely less and more is mathematical modelling for encrypting joint key, for which reason, the recursive process in encryption is reduced and system potentially updates the used key in very faster track. Hence proposed system is observed with less time complexity.

Figure 4 shows the storage complexity of the proposed and existing system. Zhang et al. [26] has adopted AES algorithm with 128 bit encryption technique along with storage of the keys in the matrix. However the proposed system is independent of any such things. Neither MTKD stores any joint key after performing encryption not it is broadcasted for which reason the storage factor is almost uniformly distributed with flexible size of keys. The proposed study is the first of its kind to exhibit the fact that it is possible to perform encryption with lower values of standard 128 bit with security options more than existing cryptographic protocols. The comparative analysis of the proposed and Zhang et al. [26]

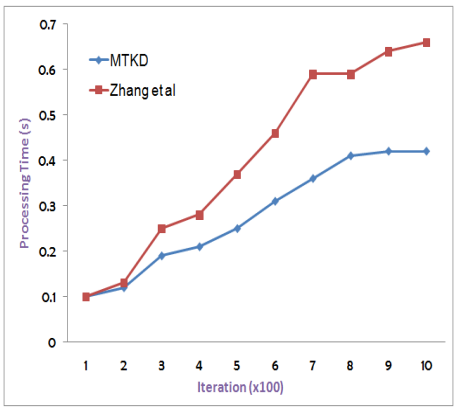

Figure 3. Analysis of Time Complexity

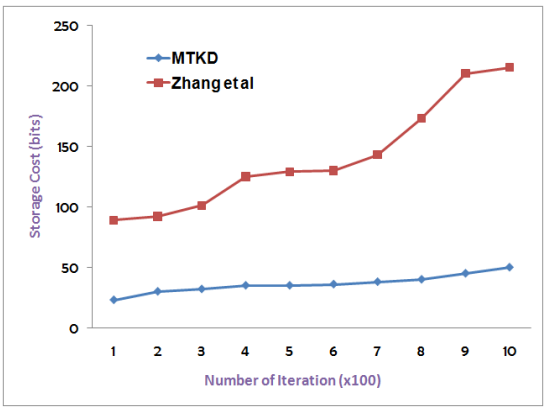

Figure 4 Analysis of Storage Complexity

Table 1 Difference Between Proposed & Existing System

MTKD	Zhang et al. [26]
Focuses On Node Capture Attack, Denial-Of-Service, Tunneling Attack, Sybil attack	Focuses on Node capture attack
Uses flexible key size < or > 128 bit depending on the requirement	Uses 128 bit of key
Security incorporations in all the stages of communications (n-Tier)	Security incorporations in only group communication (1-tier)
Stores only group key (preloaded) to perform group communication, Doesn't store Joint key.	Stores seeds of key in mesh client
No need to perform broadcasting key information to extract Joint key	Broadcast keys information

8. CONCLUSION

Cryptography plays a critical role in performing encryption retaining the data and channel security. It has also contributed to strengthen the group communication in wireless sensor network. Whether it is insider or outsider attack, it significantly affects the performance of the security protocol. Hence, we have carried out almost all the recent standard work in the line of security in group communication and found that there are various techniques to strength group communication system. However, we have not came across much significant idea that considers both group communication as well as data aggregation process in wireless sensor network.

REFERENCES

[1] N.Meghanathan, S. Boumerdassi, N. Chaki, D. Nagamalai, "Recent Trends in Network Security and Applications: Third International Conference", *The Third International Conference on Network Security and Applications*, 2010

[2] R.Shyamala, S. Valli, "Impact of Black hole and Rushing Attack on the Location-Based Routing Protocol for Wireless Sensor Networks", *Advance in Computer & Inform, Technology*, pp. 349-359, 2012

[3] T. Shimeall, J. Spring, "Introduction to Information Security: A Strategic-Based Approach", *Newnes Compute*, pp. 382, 2013

[4] J.Sen, "Security and privacy challenges in cognitive wireless sensor networks", arXiv preprint arXiv: 1302.2253, 2013

[5] G. Sharmaa, S. Balaa, A.K.Vermaa, "Security Frameworks for Wireless Sensor Networks-Review", *2nd International Conference on Communication, Computing & Security*, SciVerse Science Direct, 2012

[6] C. Cheikhrouhou, A. Koubâa, G. Dini, and M. Abid, "RiSeG: a ring based secure group communication protocol for resource-constrained wireless sensor networks", *Personal and Ubiquitous Computing*, Vol. 15, No. 8, pp. 783-797, 2011

[7] W.Bechkit, Y. Challal, and A. Bouabdallah, "A new scalable key pre-distribution scheme for wsn." In *Computer Communications and Networks (ICCCN)*, 21st International Conference, pp. 1-7, 2012

[8] S.Khalid, F.Ahmad, and M. R. Beg, "Secure Key Pre-distribution in Wireless Sensor Networks Using Combinatorial Design and Traversal Design Based Key Distribution", *International Journal of Smart Sensors and Ad Hoc Networks* (IJSSAN), Vol.1, Iss.4, 2012

[9] Q.Mi, J.A. Stankovic, and R. Stoleru, "Practical and secure localization and key distribution for wireless sensor networks", *Ad Hoc Networks*, Vol. 10, No. 6, pp. 946-961, 2012

[10] L.B.Oliveira, M. Scott, J. Lopez, and R. Dahab, "TinyPBC: Pairings for authenticated identity-based non-interactive key distribution in sensor networks", *Computer Communications*, Vol. 34, No. 3, pp. 485-493, 2011

[11] P.P-Sanchez, J.E. Tapiador, P.P-Lopez, and G. S-Tangil, "Secure Publish-Subscribe Protocols for Heterogeneous Medical Wireless Body Area Networks", *Sensors*, Vol. 14, No. 12, pp.22619-22642, 2014

[12] R.Bellazreg and N. Boudriga, "DynTunKey: a dynamic distributed group key tunneling management protocol for heterogeneous wireless sensor networks", *Wireless Communication and Networking*, 2014

[13] O. G-Morchon, R. Rietman, L. Tolhuizen, *"HIMMO-A Lightweight, Fully Collusion Resistant Key Pre-Distribution Scheme*", Retrieved 2014

[14] X. Wanga, P. Lia, Y. Suia, and H. Yanga, "A Hexagon-based Key Pre-distribution Scheme for Wireless Sensor Networks", *Journal of Information & Computational Science*, Vol. 11 (8), pp. 2479-2491, 2014

[15] M. Miettinen, N. Asokan, T.D.Nguyen, A-R.Sadeghi, and M. Sobhani, "Context-Based Zero-Interaction Pairing and Key Evolution for Advanced Personal Devices", In *Proceedings of the ACM SIGSAC Conference on Computer and Communications Security*, pp. 880-891, 2014

[16] J. Furtak, and J. Chudzikiewicz, "The concept of authentication in WSNs using TPM", Computer Science and Information Systems, Vol. 3, pp. 183–190, 2014

[17] W. Xi, X-Y. Li, C. Qian, J. Han, S. Tang, J. Zhao, and K. Zhao, "Keep: Fast Secret Key Extraction Protocol for D2D Communication", *IEEE*, 2014

[18] M. Masdari and M. Tanabi, "Multipath Routing protocols in Wireless Sensor Networks: A Survey and Analysis", *International Journal of Future Generation Communication and Networking*, Vol.6, No.6, pp.181-192, 2013

[19] M.Radi, B.Dezfouli, K.A.Bakar, and M.Lee, “Multipath routing in wireless sensor networks: survey and research challenges", *Sensors*, Vol. 12, No. 1, pp.650-685, 2012

[20] D. Mittal, S. Kaur, “Enhanced Location-Aware Routing Protocol for Wireless Sensor Network”, *International Journal of Science and Modern Engineering (IJISME)*, Vol. 1, Issue. 12, 2013

[21] C.Reardon, A.D.Falco, K.Welna, and T. Krauss, "Optical beam-steering for wireless sensor networks", In *LEOS Annual Meeting Conference Proceedings, LEOS*, pp. 583-584, 2009

[22] M.I.Afzal, W.Mahmood, S.M. Sajid, and S. Seoyong, "Optical wireless communication and recharging mechanism of wireless sensor network by using CCRS", *International Journal of Advance Science and Technology*, Vol. 13, 59-68, 2009

[23] H. Chan, A. Perrig, and D. Song, "Random key predistribution schemes for sensor networks", In *Security and Privacy*, Proceedings. Symposium, pp. 197-213, 2003

[24] H.Chan, A. Perrig, and D. Song, "Key distribution techniques for sensor networks", In *Wireless sensor networks Springer*, pp. 277-303, 2004

[25] S.A.Camtepe, and B. Yener, "*Key distribution mechanisms for wireless sensor networks: a survey*", Rensselaer Polytechnic Institute, Troy, New York, Technical Report, 2005

[26] Y.Zhang, L. Xu, Y. Xiang, and X. Hauang, “A Matrix-Based Pairwise Key Establishment Scheme for Wireless Mesh Networks Using Pre Deployment Knowledge”, *IEEE Transaction on Emergencies Topics in Computing*, Vol. 1, No. 2, 2013