Exploratory Insights on Efficacy of Existing Key Management Techniques in Wireless Sensor Network

VANEETA M
Department of Computer Science and Engineering
K. S Institute of Technology,
Bengaluru, Karnataka, India

S. SWAPNA KUMAR
Department of Electronics & Communication Engineering
Vidya Academy of Science and Technology,
Thrissur, Kerala, India

***Abstract*— Demands of higher degree of resilient key management have been always high in any research-based solutions towards addressing security problems in Wireless Sensor Network (WSN). This paper reviewed the existing key management techniques in highly structured manner in order to understand the strength and weakness of existing system. The prime contribution of proposed system is to highlight the effectiveness of key management techniques in the form of its usage as public key-based approaches, key pre-distribution approaches, dynamic key management schemes, and hierarchical key management schemes in WSN to strengthen the security system. The proposed manuscript also offers a comprehensive visualization of existing research trends by analytical approach along with explicit highlights of potential research gap. It is believed that this paper will assists in providing a quick snapshot of effectiveness of key management techniques for enhancing security in WSN.**

Keywords- Security, Key Management, Encryption, Attacks, Key Predistribition, Wireless Sensor Network

I. INTRODUCTION

Basically, a Wireless Sensor Network (WSN) assists in capturing the essential environmental information with an aid of a sensor mote and is already reported to be utilized in various applications e.g. healthcare, industrial, habitat monitoring, defense etc. [1]. All these sensor motes are quite smaller in dimension and also possess restricted memory, computational capability, and energy to perform sophisticated sensing operation [2]. Normally, WSN is used on the area that are humanly inaccessible and therefore ensuring security to the communication system by the sensor node is quite a challenging task till date [3]. Some of the inherent problems associated with the security loopholes in WSN are as follows viz. i) resources are highly limited in sensor, ii) the density of the nodes could be high or less and in both scenario communication gets affected, iii) establishing error free communication in wireless medium is still an open end problem, iv) usage of fixed infrastructure makes the nodes highly vulnerable to trap the attention of adversary, v) unknown nature of network topology prior to deployment of nodes calls for higher degree of uncertainty for successful implementation of security protocols, and vi) increased threats of physical attacks within the nodes in WSN. Hence, security is still a basic requirements in WSN as there is no effective policy to offer better resiliency.

In existing system, there are various secure routing protocols with a set of advantages as well as limiting characteristics [4]. However, majority of the secure routing schemes uses key management schemes that are found to adopt either distributed or hierarchical approach. Existing system also uses pre-distributed, group wise or pairwise secret keys. There is also a practice of doing broadcasted, multicast, or unicasted mechanism for performing an effective key distribution in WSN. It was found that key management is the base of all the existing security techniques where ensuring the random factor of the sequences of the key is still an open challenge. There are also significant forms of security issues associated with the understanding of attacking policies along with identifying the phenomenon of anomalies. Apart from this, there has been voluminous amount of literatures being focused on addressing the problems associated with lethal threats e.g. denial-of-service [5], replication attack [6], etc. There are also various studies that have focused on attacks specific to protocol in WSN [7].

Ensuring an effective key management system is a challenging task owing to limited resources within the sensor nodes. Existing techniques mainly uses either asymmetric or symmetric encryption strategies in key management protocols where utilization of the public key based encryption is found to have displayed the defective behavior. Therefore, there is a good amount of research work towards emphasizing the key Predistribution protocols in order to minimize the cumulative cost involvement in key establishment system. However, there is still a less report of an effective work being carried out towards key management system in WSN, where flagship work of potential key management is yet to be seen in WSN.

The prime contribution of the presented manuscript is to offer existing contribution of research work being carried out towards enhancing the performance of key management system in WSN. The paper also emphasizes on the existing research

trends and identification of the existing research gap. Section 1.1 discusses about the background of the study where different review studies are discussed for security schemes in WSN followed by discussion of research problems in Section 1.2 and proposed solution in 1.3. Section 2 discusses about existing research contribution followed by discussion of existing research trend in Section 3 and brief of research gap in Section 4. Finally, the conclusive remarks are provided in Section 5.

A. Background

Although, the problems pertaining to security system in WSN aged more than a decade old, there is less amount of significant review work carried out in this direction. Most recently, the review work carried out by. [8] have discussed about existing solutions towards the security threats in wireless body area network where it explores the no applicability of existing techniques on resource constraint wireless body area network as well as it has highlighted about incapability of achieving better computational excellence in performance. Similar discussion of existing key management technique has been carried out by [9] on wireless body area network.

The review shows that almost all the protocols suffer from high computational complexity and doesn't ensure non-repudiation. [10] Have also surveyed existing approaches of key management in WSN. However, only ten frequently existing schemes has been reviewed in this work where the study outcome shows that all the presented schemes suffers from communication overhead and less retention of energy efficiency. [11] Have reviewed some of the existing key distribution scheme in WSN. The survey includes the use of the piggy bank approach to cryptography in which part of the key is pre-distributed and the remainder is varied in the application. Apart from the above mentioned studies, there is little significant literature towards reviewing the existing schemes of secure key management in WSN.

B. Research Problem

From the prior section, it can be seen that there are less number of significant studies of review work being carried out in perspective of key management techniques in WSN. With presence of very few review-based literatures, it is quite a difficult task to make out the effectiveness of existing key management techniques. The discussion made in the existing review work is quite generalized and it is quite difficult to visualize the security strength of the existing key-based security protocols in WSN. Therefore, the research problem of the proposed study will be to identify the strength and weakness of existing key management schemes in WSN from the recent implementation schemes along with the identification of significant research gap.

C. Proposed Solution

There are different variants of the existing key management techniques in WSN, where it is required to understand an efficacy of each schemes. The present study discusses about the significant research-based techniques that has been published in the duration of 2010-2017 in order to offer highly updated information about existing key management approaches. After reviewing the literatures, we found that there are highly scattered forms of work where majority of the work are interlinked with each other. Therefore, for an effective discussion, we categorize the existing system in four different classes i.e. i) studies on public-key based approach, ii) key-distribution based approach, iii) dynamic key management techniques, and iv) Hierarchical key management techniques. Finally, we discuss about the existing research trend to offer more insight towards the frequency of existing research work in the area of key management techniques followed by brief discussion of potential research gap.

II. EXISTING KEY MANAGEMENT SCHEMES IN WSN

This section discusses about the existing key management techniques adopted for securing the communication in WSN. However, the approach of key management technique have highly revolutionized in last decade into multiple forms. Therefore, this section will discuss about the different key management techniques that were frequently used in WSN. It includes only the recent and most frequently used techniques of research published during 2010-2017.

A. Schemes based on Public key

Basically, usage of public key based encryption scheme is quite frequent in WSN. The most frequently adopted techniques under this scheme are RSA algorithm and Elliptical Curve Cryptography (ECC) scheme. Most recently, usage of ECC was seen in the work of [12] for the purpose of securely disseminating grid-based data. The technique uses a spherical node deployment strategy. Emphasis on authentication problems is seen in the work of [13]. The author uses ECC-based key management technique for assisting in authentication along with usage of digital signature. [14] have implemented RSA algorithm in order to make the system design free from using any form of signature for resisting potential intrusion in WSN. [15] Have presented another public key cryptosystem using ECC where the technique offers a secure backbone network for establishing dynamic session. The simulated outcome of the study is also tested on real-time platform to find that there is a significant reduction in message overhead. [16] Have introduced the usage of the k-connectivity graphs towards enhancing the performance of public key encryption. With an aid of empirical modeling, the authors have used random k-out graphs along with its intersection.

[17] Have investigated the effect of energy on the public key encryption standard in WSN. Basically, multiple forms of public key encryption strategy have been tested in this work

that has the potential supportability of Diffie-Hellman and ECC. The study outcome shows better packet delivery ratio and energy efficiency. The performance of ECC is further enhanced as seen in the work carried out by [18] by using a scalar multiplier. The prime emphasis of the study is to obtain minimal computing time. [19] Have addressed the security issues associated with the usage of asymmetric schemes and thereby presented a solution by using ECC and Advanced Encryption Standard (AES). The scheme basically uses enhanced version of cooperative diversity for performing communication scheme where the study outcome shows reduced bit error rate performance. The study carried out by [20] has presented their claims that there is always a significant increase in computation time when scalar multiplication is applied. Therefore, this problem is addressed by applying subtraction of unit complement for providing reduced hamming weight. The core idea is to minimize the algorithm complexity during operation of scalar multiplication.

B. Key-Predistribution Schemes

Usage of such scheme permits allocations of keys well in advance using either a random scheme or certain well planned scheme to perform pre-distribution. The research work carried out by [21] investigated the resiliency of the random key predistribution and found that their presented technique is found to minimize the size of the key in heterogeneous WSN. The technique uses heterogeneous key graph in random order to construct the topology. The study towards enhancing key Predistribution protocol was also carried out by [22] in order to find the effective mechanism for securing the super network. The presented technique mainly emphasizes on the accomplishment of an equilibrium performance of the secure communication system in WSN considering small scale network. The technique also introduces a cost modeling considering the cost involved in device and deployment. The study outcome shows the feasibility of implementing the presented scheme.

[23] Have presented a technique to address the problem of node capture attack in WSN. The author investigates the q-composite mechanism and formulated a technique for enhancing the resiliency of security in sensor nodes. An analytical model is presented using random pairwise Predistribution scheme to overcome the security problem. [24] have presented a model where a key distribution is given a shape of a matrix-based operation. The technique decomposes the polynomial keypools for obtaining connectivity among the shared keys. The process then uses shared polynomial in order to compute the shared key. The presented technique is used for addressing node capture attack problems.

[25] Discuss a typical random key Predistribution technique using q-composite approach along with probability. The author uses mathematical modeling using q-composite scheme for accomplishing the security. The work carried out by. [26] have investigated the key Predistribution protocols and correlated their study with respect to node density as well as network dimension. The authors have introduced a protocol that performs scaling laws in order to retain maximum scalability. The work carried out by [27] have presented a polynomial key Predistribution that works on the basis of the key pools as well as apply probabilistic approach. The probabilistic technique is found to offer better minimization towards communication as well as memory overhead in WSN.

C. Dynamic Key Management Schemes

This technique is widely used by majority of the cryptographic approaches in WSN. However, it is still hard to make out the potential effectiveness of any existing approaches of dynamic key management. Study towards mitigating the adversarial effect of node capture attack was presented by [28] where a swarm-based optimization technique was implemented in order to enhance the security performance in WSN. The technique basically emphasize on updating the secret key using a unique network model. The study outcome shows better probability of identification of node capture attack in WSN. Literatures have also presented study towards dynamic key management considering mobile device that was used for accelerating the rate of data transmission.

The technique introduced by [29] uses symmetric encryption and hash function to incorporate security in WSN. The study outcome was analyzed considering guessing attack, replay attack, falsification attack, node capture attack, and man-in-middle attack. The work carried out by [30] has presented a dynamic key management for ensuring backward secrecy using certificate less key management technique. The technique is found to offer significant capability of key revocation process for reducing the adversarial effect on different attacks. [31] Have presented a technique that ensures security using dynamic key management using multiple levels. The technique considers an unmanned aerial vehicle to be acting as a center for performing key distribution that is configured using symmetric keys.

Joint addressing of dynamic and secure management of keys can be seen in the work carried out by [32] where the authors have implemented ECC algorithm along with signcryption approach. The technique implements periodic and a robust authentication technique in order to resist the node capture attack and desynchronization attack in WSN. [33] Have used Hamming distance for performing dynamic key management along with arbitrary distribution scheme. Usage of the mathematical modeling was seen in the work carried out by [34] for dynamic key management. The authors have used trivariate polynomial based technique in order to resist node capture attacks in WSN.

D. Hierarchical Key Management

Hierarchical key management was specially designed for addressing the energy problems associated with the implementation of security techniques in WSN. Usage of

security protocol without any certificate is carried out by. [35] along with the usage signcryption scheme for securing data aggregation. Implementation of transitory master key for designing a key negotiation protocol meant for minimizing the computational time was seen in the work of [36]. Adoption of threshold in the cryptography scheme is seen in the work of [37] where a secret sharing scheme has been adopted over multiple clusters.

[38] Have used ECC along with signcryption in order to carry out an effective key management in WSN. [39] have presented a scheme that uses location-based management of secure key in WSN along with retention of energy efficiency particularly focusing on large scale networks. All the above mentioned techniques were used for maintaining a proper balance between energy conservation within the sensor nodes as well as secure communication protocol in WSN.

Table 1 summarizes the research contribution towards key management techniques in WSN

Authors	Problem	Technique	Advantage	Limitation
Prasad [12]	Secure Communication	ECC, Spherical Node Deployment	Faster Data Delivery	Induces,Communication Overhead
Qin [13]	Authentication	ECC, Symmetric Encryption, Hash,	Reduces Energy Consumption	Induces Communication Overhead
Singh Et Al. [14]	Secure Communication	RSA	Reduced Computationally Complex	Doesn't Emphasize On Energy Efficiency
Tseng Et Al. [15]	Secure Session Establishment	ECC	Reduced Overhead	Doesn't Emphasize On Space Complexity
Yavuz Et Al. [16]	Link Security	Random K-Graph	Ensure Privacy	Doesn't Perform Comparative Analysis.
Basu And Pushpalatha [17]	Energy Efficiency In Security	Tinysec Scheme	Energy Efficient	No Applicable For Dense And Large Scale Area
Lehsaini Et Al. [18]	Enhancing Performance Of ECC	Scalar Multiplier	Reduced Computing Time	Applicable To Small Scale Network Only
Ganesh Et Al. [19]	Secure Communication	Extended Cooperative Space-Time Block Codes	Reduced BER Performance	Not Benchmarked
Huang Et Al. [20]	Enhancing ECC	Scalar Multiplication, Fuzzy Logic	Reduced Time Of Calculation	Not Benchmarked
Yagan And Makowski [21]	Heterogeneous Network, Security	Random Key Graph	Ensure Unsplitabilty Of Key	Associated With Computational Complexity For Large Network
Yuan Et Al. [22]	Heterogeneous Network, Optimizing Key Predistribution	Empirical, Cost-Based, Equilibrium	Optimizes Node Performance	No Benchmarking
Zhao [23]	Resiliency Enhancement, Node Replication Attack	Q-Composite, Empirical Approach,	Resistive Against Node Replication Attack, Enhanced Connectivity Probability	No Benchmarking
Dai And Xu [24]	Enhancing Performance Of Key Predistribution	Matrix-Based Decomposition, Mutual Authentication	Optimize Memory Overhead	Still Posses Computational Complexity, No Benchmarking
Yum And Lee [25]	Resiliency In WSN	Mathematical Modeling, Q-Composite	Efficient Uses Of Key Pool	Highly Iterative Operation Will Lead To Energy Consumption
Gu Et Al. [26]	Scalability	Node Density, Network Dimension, Scaling Laws, Physical Group Deployment	Efficient Protocol Design,	No Benchmarking
Rasheed And Mahapatra [27]	Enhancing Key Predistribution	Analytical Modeling, Mobile Sink, Polynomial Pool Based, Q-Composite	Enhanced Probability Of Secure Inclusion Of Regular Node In Routing Process	No Benchmarking
Zhang Et Al. [28]	Security, Node Capture Attack	Particle Swarm Optimization	Minimizes Overhead	No Benchmark, Limited To Small Scale Network
Chen Et Al. [29]	Dynamic Key Management	Mobile Nodes, Assymetric Encryption, Hash Function	Resistive Against Multiple Attacks	Communication Performance Not Discussed

Seo Et Al. [30]	Dynamic Key Management	Multiple Key Forms, Analytical Model	Reduces Energy Consumption	Doesn't Completely Ensures Quality Of Service
Sahingoz [31]	Dynamic Key Management	Asymmetric Keys	Efficient Key Management	No Benchmarking
Alagheband And Aref [32]	Dynamic Key Management In Heterogeneous WSN	ECC, Signcryption	Good Control On Overhead	Significant Rise Of Computational Complexity On Dense Network.
Divya And Thirumurugan [33]	Dynamic Key Management, Node Collusion	Key Assignment, Random Key Distribution	Minimizes Node Collusion	No Benchmarking
Ning Et Al. [34]	Dynamic Key Management	Trivariate Polynomial	Simplified Implementation Scheme	Doesn't Address Computational Complexity
Won Et Al. [35]	Security In Smart Cities	Sigcryption, Certificateless	Efficient Computation Time	Lacks Scalability
Gandino Et Al. [36]	Faster Computation	Transitory Master Key,	Minimized Computational Time	Doesn't Discuss About Computational Complexity
Singh And Sharma [37]	Reliability In Security Scheme	Secret Sharing	Minimizes Events Of Packet Drop	Lacks Effective Benchmarking
Hagras Et Al. [38]	Energy, Security	ECC, Signcryption	Reduces Comm. Overhead	Lower Scope In Large Network

III. QUANTITATIVE ANALYSIS OF EXISTING RESEARCH TRENDS

This section discusses about an existing research trends by performing quantitative analysis of various literatures published during 2010-2017. We emphasize more on journals as compared to conference paper and in this regard we see that Fig.1 shows more number of approaches been formulated towards addressing key Predistribution schemes followed by public key encryption in key management of WSN. Studies towards dynamic key management are quite infrequently found. There is also more number of studies being carried out towards optimizing the performance of key management.

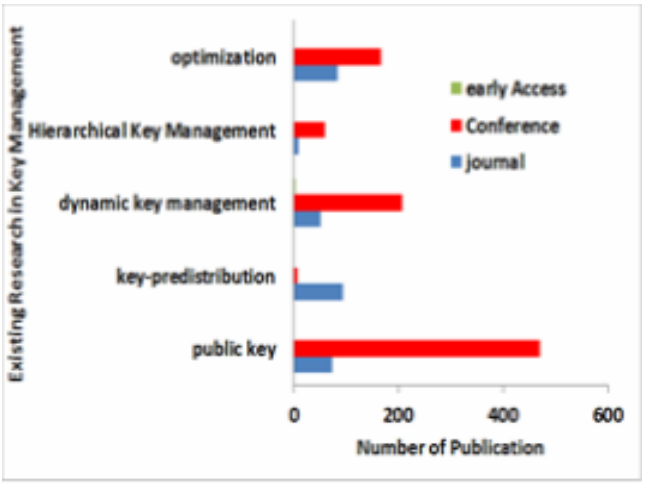

Fig 1 Research Trends in key management approaches in WSN

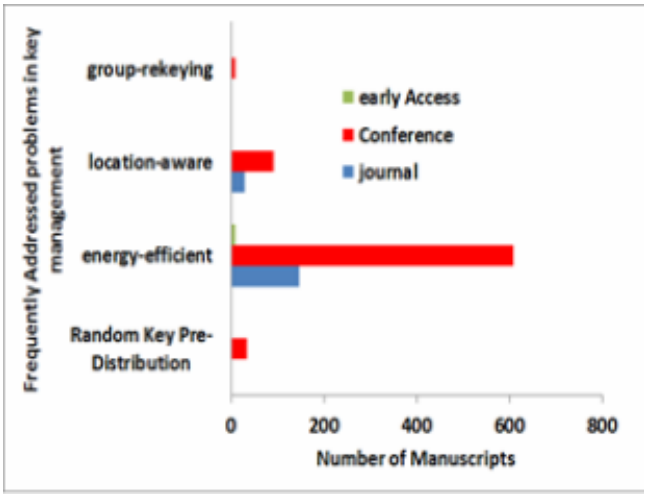

Fig 2 Research Trends to specific problems in Key Management in WSN

We also find that majority of the existing studies towards key management have been emphasizing on accomplishing energy-efficiency as shown in Fig.2. Although, there are certain degree of works being carried out towards location awareness protocol and almost no potential research being evolved since 2010 towards random key predistribution schemes as well as group rekeying scheme. From this research trend, it can be said that there has been considerable reduction in research work towards enhancing the key management schemes. Inspite of more number of works in key Predistribution scheme, there is no standard modeling yet reported for its robustness. The increasing number of research work in key Predistribution and energy efficiency only indicates the importance of these problems to be solved. At the same time, it also indicates how other problems e.g. location

awareness, group rekeying and randomness is receiving lesser attention.

V. EXISTING RESEARCH GAP

The existing research work does have associated beneficial features as well as limitation. However, we will discuss about open end problems in key management that are yet to be solved. The existing research gap is identified as follows:

A. Lesser Resistivity of Existing key Predistribution Schemes

Majority of the existing key Predistribution schemes has been presented considering different case study of adversaries where none of the case study has been actually claimed to offer computational efficiency or resource efficiency during its operation. Usage of q-composite scheme is more frequent and is characterized by significant iterative operation during the encryption. This problem has been completely overlooked that leads to security performance excellence at the cost of computational degradation.

B. Less Focus on Clustering-Based Operation

Clustering is always an essential operation in WSN. It offers energy efficiency as well as structured communication management during the data aggregation operation. Unfortunately, there are only few studies that has actually focused on clustering operation while constructing the strategies of key management techniques. Declining Focus on Authentication There is no doubt that all the key management techniques are directly assisting in authentication process among the nodes in WSN. However, the design of the algorithm in key management is actually not motivated by the real time problems incurred during authentication process e.g. identity of the nodes from different domains, link-based authentication, retaining privacy for the transmitting node during multihop operation, etc.

C. Less Improvement in Public key Encryption

All the existing techniques where public key encryption has been implemented are reported as not to do any form of upgrading the features of public key, but researchers choose to directly implement them. This causes lesser optimization and computational time increases significantly. However, slighter enhancement in features of public key encryption may save lot of computational resources which otherwise is an expensive aspect till date.

D. Ignorance to Vulnerability cause due to Mobility

There are many reported works in literature where mobile nodes are used for enhancing the transmission rate. Although, this assists in data delivery performance, but it is carried out on the basis of a mere impractical assumption. A robust authentication mechanism for mobile nodes is still missing in existing literatures. At the same time, lack of benchmarking and less focus on computational complexity is another loophole in existing research work. Therefore, there is a serious need of an effective key management technique particularly tapping more potential of pairwise key distribution in WSN.

VI. CONCLUSION

Security has been always a serious concern in wireless sensor network where existing approaches has not been completely successful towards incorporating resiliency toward lethal threats reported till date. Existing approaches towards key management techniques shows intermittent trends of research work where energy efficiency as well as pairwise key distribution has been offered more importance. This is a very viable trend as pairwise key Predistribution can significantly overcome lots of security loopholes in WSN. However, it also suffers from limitations as well as there are open end research gap which are yet to be addressed. Therefore, we will focus on investigating an effective mechanism to address such research gap in our future work and will attempt to evolve up with computationally efficient techniques that keep a good balance between computational efficiency as well as security potentials.

REFERENCES

[1] Ibrahiem M. M. El Emary, S. Ramakrishnan, “Wireless Sensor Networks: From Theory to Applications”, CRC Press, 2013

[2] H. I. Kobo, A. M. Abu-Mahfouz and G. P. Hancke, "A Survey on Software-Defined Wireless Sensor Networks: Challenges and Design Requirements," in IEEE Access, vol. 5, no. , pp. 1872-1899, 2017

[3] F. Januário, C. Carvalho, A. Cardoso and P. Gil, "Security challenges in SCADA systems over Wireless Sensor and Actuator Networks," 2016 8th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), Lisbon, 2016, pp. 363-368.

[4] I. Ouafaa, E. Mustapha, K. Salah-ddine, L. Jalal and E. H. Said, "An advanced analysis on secure hierarchical routing protocols in wireless sensor network," *2016 International Conference on Engineering & MIS (ICEMIS), Agadir*, 2016, pp. 1-6.

[5] D. Mansouri, L. Mokddad, J. Ben-othman and M. Ioualalen, "Preventing Denial of Service attacks in Wireless Sensor Networks," 2015 IEEE International Conference on Communications (ICC), London, 2015, pp. 3014-3019.

[6] B. Shimpi and S. Shrivastava, "A modified algorithm and protocol for Replication attack and prevention for Wireless sensor Networks," 2016 International Conference on ICT in Business Industry & Government (ICTBIG), Indore, 2016, pp. 1-5.

[7] A. S. Nisha, V. Vaishali, T. Shivaranjani and P. Subathra, "The effect of vampire attacks on distance vector routing protocols for wireless ad hoc sensor networks," 2016 Second International Conference on Science Technology Engineering and Management (ICONSTEM), Chennai, 2016, pp. 587-594.

[8] Shihong Zou, Yanhong Xu, Honggang Wang, Zhouzhou Li, “A Survey on Secure Wireless Body Area Networks”, Hindawi Security and Communication Networks, 2017

[9] Shaohua Chang, Sai Ji, Jian Shen,” A Survey on Key Management for Body Sensor Network”, IEEE-First International Conference on Computational Intelligence Theory, Systems and Applications, 2015

[10] A.Selva Reegan, E. Baburaj, “Key Management Schemes in Wireless Sensor Networks: A Survey”, IEEE-International Conference on Circuits, Power and Computing Technologies, 2013

[11] Pratik P. Chaphekar, “Survey of Key Distribution Schemes for Wireless Sensor Networks”, ArXiv, 2014

[12] J. P. Prasad and S. C. Mohan, "Elliptical Curve based multi-tier Spherical Grid routing model for smart & secure global communication using WSN's," 2016 IEEE 1st International Conference on Power Electronics, Intelligent Control and Energy Systems (ICPEICES), Delhi, 2016, pp. 1-6.

[13] D. Qin, S. Jia, S. Yang, E. Wang and Q. Ding, "A Lightweight Authentication and Key Management Scheme for Wireless Sensor Networks", Journal of Sensors, 2016, pp. 9.

[14] J. Singh, V. Kumar and R. Kumar, "An RSA based certificateless signature scheme for wireless sensor networks," 2015 International Conference on Green Computing and Internet of Things (ICGCIoT), Noida, 2015, pp. 443-447.

[15] C. H. Tseng, S. H. Wang and W. J. Tsaur, "Hierarchical and Dynamic Elliptic Curve Cryptosystem Based Self-Certified Public Key Scheme for Medical Data Protection," in IEEE Transactions on Reliability, vol. 64, no. 3, pp. 1078-1085, Sept. 2015.

[16] F. Yavuz, J. Zhao, O. Yağan and V. Gligor, "Toward k -Connectivity of the Random Graph Induced by a Pairwise Key Predistribution Scheme With Unreliable Links," in IEEE Transactions on Information Theory, vol. 61, no. 11, pp. 6251-6271, Nov. 2015.

[17] S. Basu and M. Pushpalatha, "Analysis of energy efficient ECC and TinySec based security schemes in Wireless Sensor Networks," 2013 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS), Kattankulathur, 2013, pp. 1-6.

[18] M. Lehsaini, M. Feham and C. T. Hellel, "Improvement of scalar multiplication time for elliptic curve cryptosystems," 2013 11th International Symposium on Programming and Systems (ISPS), Algiers, 2013, pp. 53-57.

[19] A. R. Ganesh, P. N. Manikandan, S. P. Sethu, R. Sundararajan and K. Pargunarajan, "An improved AES-ECC hybrid encryption scheme for secure communication in cooperative diversity based Wireless Sensor Networks," 2011 International Conference on Recent Trends in Information Technology (ICRTIT), Chennai, Tamil Nadu, 2011, pp. 1209-1214

[20] X. Huang, J. Campbell and F. Gao, "Scalar Multiplication of a Dynamic Window with Fuzzy Controller for Elliptic Curve Cryptography," 2010 Fourth International Conference on Network and System Security, Melbourne, VIC, 2010, pp. 600-605.

[21] O. Yagan and A. M. Makowski, "Wireless Sensor Networks Under the Random Pairwise Key Predistribution Scheme: Can Resiliency Be Achieved With Small Key Rings?," in IEEE/ACM Transactions on Networking, vol. 24, no. 6, pp. 3383-3396, December 2016.

[22] Qi Yuan, Chunguang Ma, Xiaorui Zhong, Gang Du and Jiansheng Yao, "Optimization of key predistribution protocol based on supernetworks theory in heterogeneous WSN," in Tsinghua Science and Technology, vol. 21, no. 3, pp. 333-343, June 2016.

[23] J. Zhao, "On Resilience and Connectivity of Secure Wireless Sensor Networks Under Node Capture Attacks," in IEEE Transactions on Information Forensics and Security, vol. 12, no. 3, pp. 557-571, March 2017.

[24] H. Dai and H. Xu, "Key Predistribution Approach in Wireless Sensor Networks Using LU Matrix," in IEEE Sensors Journal, vol. 10, no. 8, pp. 1399-1409, Aug. 2010.

[25] D. H. Yum and P. J. Lee, "Exact Formulae for Resilience in Random Key Predistribution Schemes," in IEEE Transactions on Wireless Communications, vol. 11, no. 5, pp. 1638-1642, May 2012.

[26] W. Gu, S. Chellappan, X. Bai and H. Wang, "Scaling Laws of Key Predistribution Protocols in Wireless Sensor Networks," in IEEE Transactions on Information Forensics and Security, vol. 6, no. 4, pp. 1370-1381, Dec. 2011.

[27] A. Rasheed and R. Mahapatra, "Key Predistribution Schemes for Establishing Pairwise Keys with a Mobile Sink in Sensor Networks," in IEEE Transactions on Parallel and Distributed Systems, vol. 22, no. 1, pp. 176-184, Jan. 2011.

[28] Zhang Y, Zheng B, Ji P, Cao J. A key management method based on dynamic clustering for sensor networks. International Journal of Distributed Sensor Networks. 2015 Jul 1;11(7):763675.

[29] Chen CL, Chen CC, Li DK. Mobile device based dynamic key management protocols for wireless sensor networks. Journal of Sensors. 2015 Aug 16;2015.

[30] S. H. Seo, J. Won, S. Sultana and E. Bertino, "Effective Key Management in Dynamic Wireless Sensor Networks," in IEEE Transactions on Information Forensics and Security, vol. 10, no. 2, pp. 371-383, Feb. 2015.

[31] Sahingoz OK. Multi-level dynamic key management for scalable wireless sensor networks with UAV. In Ubiquitous Information Technologies and Applications 2013 (pp. 11-19). Springer Netherlands.

[32] M. R. Alagheband and M. R. Aref, "Dynamic and secure key management model for hierarchical heterogeneous sensor networks," in IET Information Security, vol. 6, no. 4, pp. 271-280, Dec. 2012.

[33] R. Divya and T. Thirumurugan, "A novel dynamic key management scheme based on hamming distance for wireless sensor networks," 2011 International Conference on Computer, Communication and Electrical Technology (ICCCET), Tamilnadu, 2011, pp. 181-185.

[34] J. Ning, X. Yin and T. Yang, "A Trivariate Polynomial-based Dynamic Key Management Scheme for Wireless Sensor Networks," 2011 Seventh International Conference on Computational Intelligence and Security, Hainan, 2011, pp. 625-629.

[35] J. Won, S. H. Seo and E. Bertino, "Certificateless Cryptographic Protocols for Efficient Drone-Based Smart City Applications," in IEEE Access, vol. 5, no. , pp. 3721-3749, 2017.

[36] F. Gandino, R. Ferrero, B. Montrucchio and M. Rebaudengo, "Fast Hierarchical Key Management Scheme With Transitory Master Key for Wireless Sensor Networks," in IEEE Internet of Things Journal, vol. 3, no. 6, pp. 1334-1345, Dec. 2016.

[37] Kamaljit Singh, Lalit Sharma, "Hierarchical Group Key Management using Threshold Cryptography in Wireless Sensor Networks", International Journal of Computer Applications (0975 – 8887) Volume 63– No.4, February 2013

[38] E. A. A. A. Hagras, D. El-Saied and H. H. Aly, "Energy efficient key management scheme based on elliptic curve signcryption for Wireless Sensor Networks," 2011 28th National Radio Science Conference (NRSC), Cairo, 2011, pp. 1-9.

[39] L. He, Y. Y. Zhang, L. Shu, A. V. Vasilakos and M. S. Park, "Energy-Efficient Location-Dependent Key Management Scheme for Wireless Sensor Networks," 2010 IEEE Global Telecommunications Conference GLOBECOM 2010, Miami, FL, 2010, pp. 1-5.

AUTHORS PROFILE

Vaneeta M is Associate Professor in Department of Computer Science and Engineering, K. S Institute of Technology, Bengaluru, Karnataka, India. She received B.E degree in Department of Computer Science and Engineering from Dr. BAMU University, Maharashtra and M.E degree in Department of Computer Science and Engineering, Anna University. She is currently pursuing her Ph.D. degree in the Department of Computer Science and Engineering, Visvesvaraya Technological University, Belagavi. Her research interests include wireless sensor networks, secure communication networks and Image processing.

S. SWAPNA KUMAR, Ph.D., is Professor and Head of Department of Electronics and Communication Engineering, in Vidya Academy of Science and Technology, Thrissur, Kerala, India. Presently, he is a Supervisor for the Ph.D. scholars under Visvesvaraya Technological University (VTU) and also an external examiner for Thesis evaluation/ Public Viva-voce of Ph.D. students. He has been in the teaching for profession courses under UG/PG level for nearly decade, and has worked for various national and international industries.He is a reviewer of several National and International journals. Besides, he has also authored a books on ``A Guide to Wireless Sensor Networks'' and ``MATLAB easy way of learning''. Dr. Swapna Kumar is a Fellow Member and Chartered Engineer of the Institution of Engineers (INDIA). He has also a life membership of several professional bodies, including Indian Society for Technical Education (ISTE) and IEEE. His area of interest include Networking, Security system, Fuzzy Logic, Data Communication, Electronics, Communication Systems, Embedded Systems, MATLAB modeling and simulation.