IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-7, Issue-3, March 2019 E-ISSN: 2347-2693

# A Hybrid Key Management Scheme for Data Transmission in Wireless Sensor Networks

**M. Infant Ange[1]*, R.Sudha[2]**

[1]Dept. of Computer Science, Park's college, Tirupur, India
[2]Dept. of Computer Science, PSG College of Arts &Science, Coimbatore, India

*Corresponding author: infantangel2196@gmail.com*

DOI: https://doi.org/10.26438/ijcse/v7i3.787793 | Available online at: www.ijcseonline.org

Accepted: 06/Mar/2019, Published: 31/Mar/2019

***Abstract*:** In Wireless Sensor Networks (WSNs), many application scenarios, traditional WSNs with static sink nodes will be replaced by Mobile Sinks (MSs), and also the corresponding application needs secure communication surroundings. Key Management is that the most crucial issue within the security of Wireless detector Networks. Current key management researches pay less concentration to the safety of detector networks with MS. This paper proposes a hybrid key management system supported a Polynomial Pool-based key pre-distribution and Basic Random key pre-distribution (PPBR) to be working in WSNs with Mobile Sink. The system takes full remuneration of those two sorts of ways to boost the excellent problem of the key system. It constructs the oppose have to be compelled to capture a big range of nodes within the network to decrypt the keys since it is to have the polynomial coefficients and random keys at a corresponding time so as to confine the uncompromised nodes. The encryption procedure is performed by utilizing an AES algorithm. Message digest algorithm is used for key generation. Simulation evidently shows that the theme of the research work performs higher in terms of network resilience, property and storage effectiveness compared to alternative wide used schemes.

***Keywords*:** Wireless sensor networks, Hybrid key, Polynomial pool based key, Basic random key

## I. INTRODUCTION

Wireless sensor networks (WSN) become more and more widespread, the safety and irresponsibleness problems attract additional and additional attention. because of the broadcasting and open nature of wireless mediums, WSN a susceptible to identity-based spoofing attacks, wherever an unauthorized user tries to impersonate another legitimate user to realize illegitimate benefits. Identity-based attacks a terribly straightforward to launch and a thought-about because the start for attackers launching varied varieties of attacks like session hijacking, denial of service (DOS) and man-in-the-middle [11]. for instance, in goods networks, like 802.11 networks, it's straightforward for a tool to change its Media Access Management (MAC) address a claim to another one by mere mistreatment an "if config" command.

Hence, the power completely differentiates to tell apart between different transmitters would be notably valuable for preventing spoofing attacks. Authentication is an efficient approach to manage such identity-based attacks, by that the meant receivers will verify the identities of concerned sending users and certify that the received knowledge return from the expected user [34]. An ancient authentication mechanism is handled at the upper-layer mistreatment key-based cryptography.

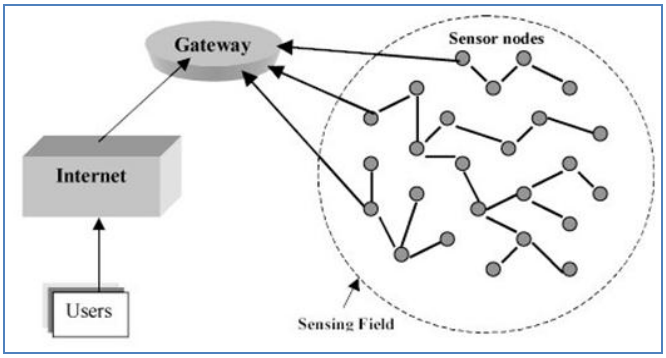


**Figure 1.1: WSN Architecture**

Figure 1.1 shows the architecture of the WSN. The most reduced level comprises of the sensor nodes that do broadly useful figuring furthermore, organizing in spite of application-particular detecting. The sensor nodes might be conveyed in thick fixes that are generally isolated. The sensor nodes send their information through the sensor system to the sensor arrange gateway. The gateway is in charge of transmitting sensor information from the sensor fix through a nearby travel arrange to the remote base station that gives WAN availability, what's more, information logging. The base station interfaces with database reproductions over the web. At last, the information shown is to researchers through a User Interface.

 

Key management is one in all the vital security aspects of WSNs because it is crucial for providing knowledge authentication, confidentiality and integrity and the majority WSN security mechanisms accept solid secret writing. even supposing key management has been intensively studied in broadcast communication and isn't a singular issue to wireless sensing element networks, ancient key management techniques can't be used for WSNs directly or perhaps with minor revision thanks to the constraints of sensing element nodes and application environments. Centro symmetric Key Cryptography based mostly techniques an engaging for WSN application as a result of their energy-efficient

A main objective is to produce higher key management mechanism exploitation the PPBR theme. It assigns completely different variety of polynomials and keys in MS and detector nodes to create the polynomial ring, and therefore the heterogeneousness of PPBR can improve its security performance compared to the homogeneity of the amar theme. Additionally, compared to the strategy of communication link institution solely supported likelihood within the Amar theme, the tree-based path key institution methodology within the PPBR theme will improve the property likelihood of building communication links. We use the tree-based methodology to determine the trail key for key management. It will establish a dynamic indirect communication link between the MS and therefore the detector nodes UN agency cannot communicate with the MS directly. The dynamic tree-based path key institution will improve the key property for key management of the network. These sorts of themes may be classified as key pre-distribution scheme supported polynomials, and their objective is to determine a novel session key for any 2 nodes underneath the condition of getting identical polynomial

## II. EXISTING METHODOLOY

Many key management schemes were projected for safeguarding wireless sensing element networks (WSNs). Whereas applying key management to the network, it's vital to confirm that the potency of the network isn't greatly plagued by key property. Poor property may result in several messages forwarding. Consequently, an oversized quantity of energy of the concerned nodes would be consumed throughout message forwarding, that isn't appropriate for the resources-constraint sensing element nodes. During this work, we have a tendency to analyze the impact of key property on the potency of communication. Then, a unique key generation methodology supported system of equations is projected to enhance key property of key management. The concerned equations are applied to ascertain secret keys and every node uses these keys for safeguarding their communication.

Several issues have to be compelled to be considered: 1) the authentication of relay nodes; 2) resources consumption of all concerned nodes (including relay nodes) caused by the messages forwarding, i.e., resource-constraint relay nodes have to be compelled to consume their precious resources to finish the communication, like energy, information measure and memory.

## III. RELATED WORKS

Swapna Naik et al [21] WSN consists of a huge type of detector Nodes where each detector Nodes inside the network are connected by a wireless channel. The node will sense the environmental data and sends to the other detector nodes or Base Station. Throughout the transmission of information from one node to a distinct node, fully totally different security techniques are used. To implement security, like confidentiality, integrity and authentication, keys are needed. Key Management is extremely necessary for implementing security in AN extremely wireless detector Network.

Mahmood Khalel et al [24] points out Diffie-Hellman algorithmic rule are liable to the man-in-the-middle attack within which the offender browse to read and modify all messages between Alice and Bob., The man-in-the-middle attack is prevented by a station-to-station key agreement by victimisation a digital signature with public key certificates to determine a session key between Alice and Bob. A changed version victimisation zero data with Diffie-Hellman is usually recommended wherever a sure third party selects 2 prime numbers p and g, and announces them as public numbers.

Samantkhajuria et al [25] have bestowed changed version of Diffie- Hellman. It's enforced victimisation Elliptic Curve Cryptography (ECC) over GF (2m) so as to get stronger cryptography. During this paper victimisation curves and TNAF ( Tadic non-adjacent form) with partial reduction modulo. A Diffie-Hellman key exchange is enforced.

Yi Ren, Member, IEEE, et al [1] discussed unattended Wireless detector Networks (UWSNs) are defined by long periods of disconnected operation and stuck or irregular intervals between sink visits. The absence of an internet certain third party implies that existing WSN trust management schemes do not appear to be applicable to UWSNs. Throughout this work, propose a trust management theme for UWSNs to provide economical and durable trust info storage and trust generation. For trust info storage, use a geographic hash table to identify storage nodes and to significantly decrease storage value.
R. Sudha et al [32] discussed a new biometric fusion based trusted anonymous secured routing protocol which assures prevention against such attacks. More specifically, the route

 

request packets were authenticated by an iris fused with DNA coding to generate a dynamic complex group signature and to secure beside possible active attacks exclusive of presenting the node identities. In addition this work also prevented revealing real destination to intermediate nodes by adapting key-encrypted pairing onion. Simulation results confirmed the efficacy of the projected BFTASR protocol with enhanced performance as evaluated with the existing protocols.

Yang Xiao et al [33] discussed Wireless device networks have many applications, vary in size, and are deployed during a very good selection of areas. They are generally deployed in all probability adverse or even hostile setting so as that there are problems on security issues in these networks. This paper, provide a survey of key management schemes in wireless device networks. No key distribution technique is nice to any or all the things where device networks are used; therefore the techniques used ought to rely upon the requirements of target applications and resources of each individual device network.

R.Sudha et al [36] discussed novel encryption and signature scheme based on a CP_ABE algorithm. The message is intended to be perused by a gathering of clients that fulfil certain entrance control governs in a BAN. CP_ABE and MD5 calculation assume an imperative job with the end goal to play out the information transmission in a safe way.

Zhou Y.et al [31] analyzed nodes in a very device network is also lost thanks to power exhaustion or malicious attacks. To increase the time period of the device network, new node readying is critical. This paper, propose AN access management protocol supported Elliptic Curve Cryptography (ECC) for device networks. Our access management protocol accomplishes node authentication and key institution for brand spanking new nodes.

## IV. PROPOSED METHODOLOGY

A hybrid key management theme (PPBR scheme) supported a polynomial pool-based key pre-distribution and basic random key pre-distribution were accustomed propose. The theme combines the benefits of the 2 protocols, utilizes the time-degree property of polynomials and improves the protection of the normal basic random key pre-distribution theme. It makes the antagonist got to capture an oversized variety of nodes within the network to decrypt the keys, since it's to possess the polynomial coefficients and random keys at constant time so as to capture the uncompromised nodes

## V. HYBRID KEY MANAGEMENT APPROACH

A hybrid key management approach is that the plenty of increased security theme that's acceptable for static device networks. This research work proposes a hybrid key management theme (PPBR scheme) supported a polynomial pool-based key pre-distribution and basic random key pre-distribution. The theme combines the advantages of the two protocols, utilizes the t-degree property of polynomials and improves the protection of the traditional basic random key pre-distribution theme. It makes the opponent have to be compelled to capture associate degree outsized vary of nodes at intervals the network to decode the keys since it's to possess the polynomial coefficients and random keys at the same time therefore on capture the uncompromised nodes [2].

## VI. POLYNOMIAL POOL BASED RANDOM KEY METHODS

PPBR theme establishes the communication link supported an explicit likelihood, therefore there are some nodes which cannot be ready to communicate with the MS node, and this can scale back the network property. It should establish an indirect communication link within the path key institution section once the MS and detector nodes cannot establish a session key directly. The trial key institution methodology utilized in this text is completely different from the standard polynomial key management theme, and it utilizes the tree-based construction methodology in wireless detector networks. It builds a tree that regards the sink node as a root at intervals the scope of the sink node's communication. The initial values of standing and depth are all z .

In Figure 4.2 shows the server generates polynomial pool *p* including *Sp t*-degree bivariate polynomials.

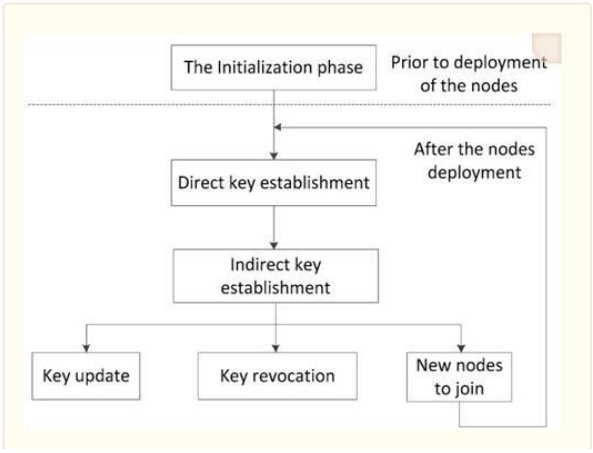


**Figure 1.2: polynomial bool based key architecture**

## VII. AES ALGORITHM

**AES Encryption process:**

The encryption period of AES can be broken into three stages: the underlying round, the principle rounds, and the last round.

 

**Initial Round**

- Add Round Key

**Main Rounds**

- Sub Bytes
- Shift Rows
- Mix Columns
- Add Round Key

**Final Round**

- Sub Bytes
- Shift Rows
- Add Round Key

## VIII. AES DECRYPTION

To decrypt an AES-encrypted cipher text, it is important to fix each phase of the encryption task in the turnaround request in which they were connected. The three phase of decryption are as per the following

**Inverse Final Round**

- Add Round Key
- Shift Rows
- Sub Bytes

**Inverse Main Round**

- Add Round Key
- Mix Columns
- Shift Rows
- Sub Bytes

**Inverse Initial Round**

- Add Round Key

## IX. MD5 ALGORITHM

Message Digest algorithm calculation takes as info a message of subjective length and produces as yield a 128-piece "unique mark" or "message process" of the information. It is guessed that it is computationally infeasible to deliver two messages having a similar message process, or to create any message having a given prespecified target message process. The MD5 calculation is expected for advanced mark applications, where a the expansive document must be "compacted" in a safe way before being encoded with a private (mystery) key under an open key cryptosystem for example, RSA.

## X. RESULTS AND DISCUSSION

The Figure 1.3 shows the energy efficiency. This graph proposed that the energy of Associated EBS is one step ahead than Normal EBS. . Let x represent the amount of neighbouring nodes around a detector and n be the amount of polynomial functions. every detector node has x storage units for the try wise keys, not + n. storage units for the t-degree polynomial functions, 2 storage units for random variety and pseudo random perform and single storage unit to store the cluster key. In terms of memory demand to store keys for every theme, the planned theme wants less memory, thus it provides measurability

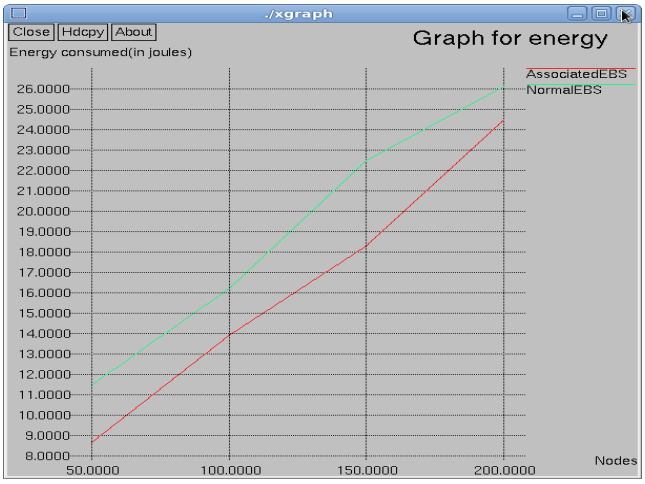


**Figure 1.3 Energy consumption**

In the BA protocol, authentications of SB messages are delayed. Somebody will exploit this characteristic and flood network with pretend messages. As a result of nodes will solely distinguish between legitimate and imitative messages once arrival of message five, they need to buffer all received messages. This might exhaust memory of nodes and stop them from running alternative tasks. To demonstrate impact of this attack we assumed that somebody chooses his time of attacks consistent with a homogenous distribution**.**

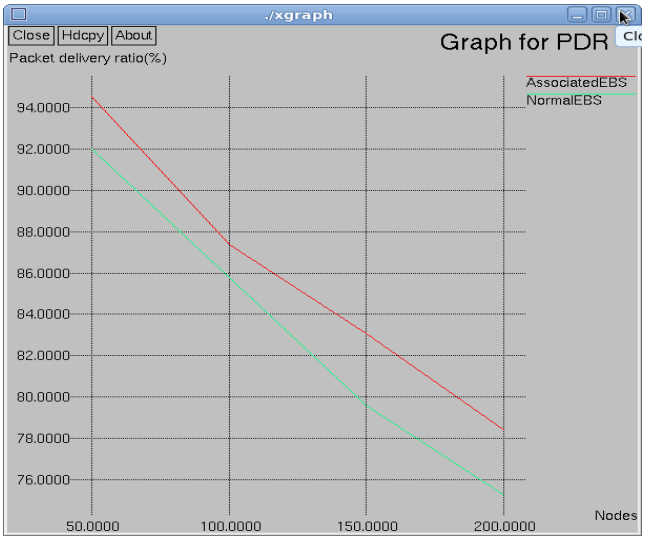


**Figure 1.4: Packet Delivery Ratio**

 

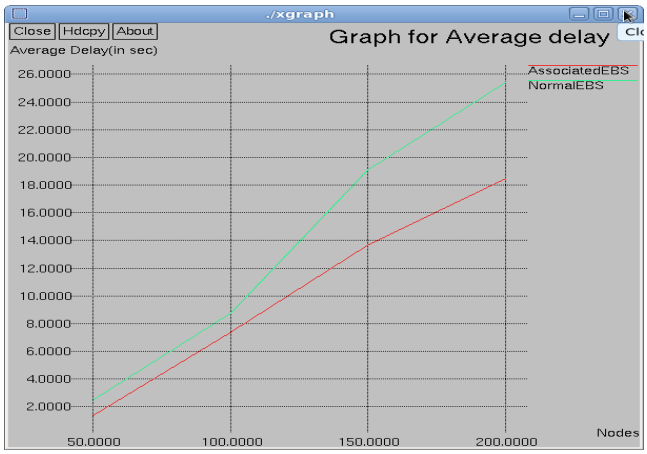


**Figure 1.5: Delay calculation**

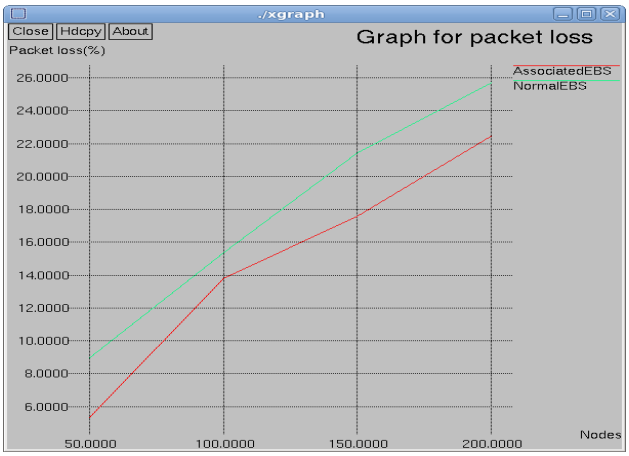


**Figure 1.6: Packet loss**

Figure 1.5 shows the delay calculation.The paket delay is very less than compared to normalEBS.

Sensor nodes will directly or indirectly build a link to a MS. once a spherical of information assortment, detector nodes will notice AN applicable tree-based path to determine communication links with the MS despite what changes within the topology occur, as well as nodes' death, the addition of latest nodes, or dynamic changes within the intermediate nodes. For a brand new spherical of information assortment, the detector nodes will follow the steps within the theme higher than.

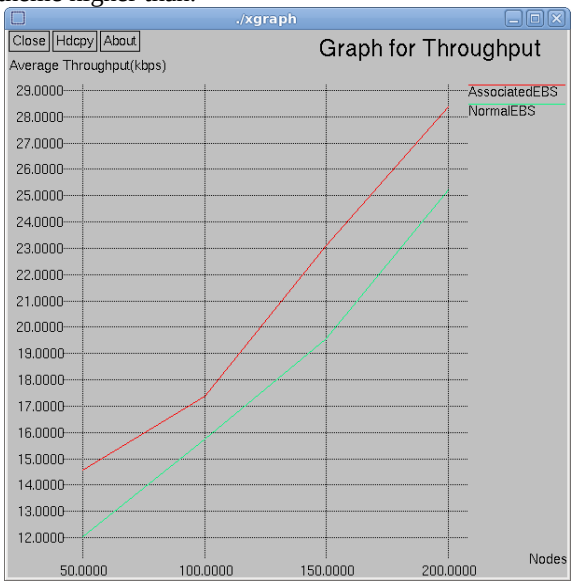


**Figure 1.7: Throughput**

Resilience is a crucial safety performance index in a very key management theme. It indicates the likelihood of the exposure of the session keys among the remaining uncompromised nodes once a number of the nodes are captured. The planned key management theme forms a polynomial pool with the key pool. It makes full use of the edge character within the polynomial key theme, and it makes the somebody have to be compelled to crack each the polynomial coefficients and also the shared keys at the same time once an outsized variety of nodes are captured, before it will influence the opposite uncompromised nodes. This greatly enhances the strength of the whole network. Commonly the MS is safe, however an outsized variety of fastened detector nodes have the danger of being captured. If there are x captured nodes, the likelihood primary key that the key within the hoop may be captured in any try of uncompromised nodes.

## XI. CONCLUSION

Wireless detector Networks (WSN) utilized in a spread of applications are sometimes unattended in nature and are extremely vulnerable to attacks like eavesdropping, hardware change of state and false messages. For secure communication among the nodes, Secret key cryptography is employed since it provides high security with low computing power. Planned theme takes full blessings of those two sorts of ways, and comprehensively considers numerous performances of the system. It will modify use of the heterogeneousness between the normal detector nodes and Mobile Sink to save lots of the space for storing of the normal detector nodes by adequately increasing the storage utilization rate of the Mobile Sink on the premise of satisfying an explicit property. In future work, more contemplate the advanced mobile network model. It suggests that more extend this theme to the networks with mobile detector nodes, not solely mobile sink nodes.

 

## REFERENCES


[1]. Yi Ren, Member, IEEE, Vladimir I. Zadorozhny, Senior Member, IEEE,Vladimir A. Oleshchuk, Senior Member, IEEE, and Frank Y. Li, Senior Member, IEEE, "A Novel Approach to Trust Management in Unattended Wireless Sensor Networks" IEEE transactions on mobile computing, vol. 13, no. 7, July 2014

[2]. Xiaojiang Du, North Dakota State University Hsiao-Hwa Chen, National Cheng Kung University "Security In Wireless Sensor Networks", IEEE wireless communications August 2008.

[3]. Chen X. MakkiK.Yen K. and Pissinou N. 'Sensor network security: A survey', IEEE Commun. Surv. Tuts, vol. 11, no. 2, pp. 52–73Apr./Jun. 2009.

[4]. Zhou Y. Zhang Y. and Fang Y. 'Access control in wireless sensor networks', Ad Hoc Netw, vol. 5, no. 1, pp. 3–13 May 2007.

[5]. Kwon T, Hong J. Learning on the job: Secure and Efficient Broadcast Authentication in Wireless Sensor Networks. IEEE Transactions on Computing. 2010 Jun 24; 59(8):1120– 33.

[6]. Khan AS, Fisal N, Bakar ZA, Salawu N, Maqbool W, Ullah R, Safdar H. Secure Authentication and Key Management Protocols for Mobile Multihop WiMAX Networks. Indian Journal of Science and Technology. 2014 Mar; 7(3):282–95.

[7]. Klaoudatou E, Konstantinou E, Kambourakis G, Gritzalis S. A Survey on Cluster-Based Group Key Agreement Protocols for WSNs. IEEE Communications Surveys & Tutorials. 2011; 13(3).

[8]. Zhang J, Varadharajan V. Learning on the job: Wireless sensor network key management survey and taxonomy. Journal of Network and Computer Applications. 2010 Mar; 33(2):63–75.

[9]. Varma AGNS, Reddy AKG, Theja RY, Arunkumar T. Cluster Based Multipath Dynamic Routing (CBDR) Protocol for Wireless Sensor Networks Indian Journal of Science and Technology. 2015 Jan; 8(S2):17–22.

[10]. Simplicio-Jr MA, Barreto PS, Margi CB, Carvalho TC. A survey on key management mechanisms for distributed wireless sensor networks. Computer Networks. 2010 Oct 28; 54(15):2591–612.

[11]. Shang F, Abolhasan M, Wysocki T. An Energy-Efficient adaptive Clustering Algorithm for Wireless Sensor Networks. International Journal of Information Acquisition. 2009; 6(2):117–26.

[12]. Gomathi K, Parvathavarthini B. An Enhanced Distributed Weighted Clustering Routing Protocol for Key Management. Indian Journal of Science and Technology. 2015 Feb; 8(4):342.

[13]. Yuhua L, Yongfeng Z, Jingju GA. New Clustering Mechanism Based on LEACH Protocol. Proceedings of the International Joint Conference on Artificial Intelligence. IEEE Communications Society; 2009 Apr. p. 25–6.

[14]. Liu D, Ning P, Li R. Establishing Pairwise Keys in Distributed Sensor Networks Proceedings 10th ACM Conference Computers and Communication Security; 2003. p. 52–61.

[15]. Diffie, W., Hellman, M. 1976. New direction in cryptography. IEEE Trans. on Info. Theory, Vol. IT-22, Nov. 1976, pp. 644-654 (Invited Paper).

[16]. Eltoweissy, M., Heydari, H., Morales, L., and Sadborough, H. 2004. Combinatorial Optimization of Group Key Management, J. Network and Systems Management 12(1), 33-50.

[17]. Eschenauer, L. and Gligor, V. D. 2002. A key-management scheme for distributed sensor networks. In Proceedings of the 9th ACM Conference on Computer and Communications Security (Washington, DC, USA, November 18 - 22, 2002).

[18]. V. Atluri, Ed. CCS '02. ACM, New York, NY, 41-47. DOI= http://doi.acm.org/10.1145/586110.586117.

[19]. Ghumman, K. 2006. Location-Aware Combinatorial Key Management Scheme for Clustered Sensor Networks. IEEE Trans. Parallel Distrib. Syst. 17, 8 (Aug. 2006), 865- 882. DOI= http://dx.doi.org/10.1109/TPDS.2006.106

[20]. P. LourduGracy, D. Venkatesan, "An Honey Encryption Based Efficient Security Mechanism For Wireless Sensor Networks". Volume 118 No. 20 2018, 3157-3164, IJPAM, 2018.

[21]. Swapna Naik, "A Novel Authentication approach in Wireless sensor Network Swapna Naik ", International Journal of Scientific & Engineering Research, Volume 5, Issue 3, March-2014

[22]. Manish P. Gangawane," Implementation Of Zero Knowledge Protocol In Wireless Sensor Network for prevention Of Various Attacks," International Journal of Emerging Technology and Advanced Engineering , (ISSN 2250-2459, Volume 2, Issue 8, August 2012).

[23]. A Jayanthiladevi, S Suma and T.Lalitha, "Challenges and Authentication in Wireless Sensor Networks," 2013 IEEE.

[24]. Mahmood Khalel, Ibrahem and Al Nahrain," Modification of Diffie–Hellman Key Exchange Algorithm for Zero Knowledge Proof," proceedings of 2012 international conference on future c ommunication networks, IEEE 2012.

[25]. SamantKhajuria and Henrik Tange, "Implementation of Diffie-Hellman Key Exchange on Wireless Sensor Using Elliptic Curve Cryptography," proceedings of IEEE 2009.

[26]. L. B. Jivanadham ,A.K.M. ,M. Islam2 and Mansoor3,"A Secured Dynamic Cluster-Based Wireless Sensor Network Advanced Informatics School (AIS)," proceedings of 2012 Fourth International Conference on Computational Intelligence,

[27]. Xiaoyong Li, Feng Zhou, and JunpingDu,"LDTS: A Lightweight and Dependable Trust System for Clustered Wireless Sensor Networks",IEEE transactions on information forensics and security, vol. 8, no. 6, June 2013

[28]. Yi Ren, Member, IEEE, Vladimir I. Zadorozhny, Senior Member, IEEE,Vladimir A. Oleshchuk, Senior Member, IEEE, and Frank Y. Li, Senior Member, IEEE, "A Novel Approach to Trust Management in Unattended Wireless Sensor Networks" IEEE transactions on mobile computing, vol. 13, no. 7, July 2014

[29]. Guoxing Zhan, Weisong Shi, Senior Member, IEEE, and Julia Deng. IEEE "Design and Implementation of TARF: A Trust-Aware Routing Framework for wsns", transactions on dependable and secure computing, vol. 9, no. 2, March/April 2012.

[30]. Chen X. Makki K.Yen K. and Pissinou N. 'Sensor network security: A survey', IEEE Commun . Surv. Tuts, vol. 11, no. 2, pp. 52–73Apr./Jun. 2009.

[31]. Zhou Y. Zhang Y. and Fang Y. 'Access control in wireless sensor networks', Ad Hoc Network, vol. 5, no. 1, pp. 3–13 May 2007.

[32]. Sudha.R, Devapriya.M," Enhanced bio-trusted anonymous authentication routing technique of wireless body area network ",Biomedical Research 2016; Special Issue: S276-S282 , Special Section: Computational Life Science and Smarter Technological Advancement, ISSN 0970-938X.

[33]. Yang Xiao, "A survey of key management schemes in wireless sensor networks", 2007 Elsevier B.V. All rights reserved. doi:10.1016/j.comcom.2007.04.009

[34]. Syed Muhammad et al, "Key Management Schemes of Wireless Sensor Networks: A Survey" ,http://uclab.khu.ac.kr

[35]. A.Pranusha , "A Hybrid Key Management Scheme For Secure Manet Communications", eISSN: 2319-1163 | pISSN: 2321-7308

[36]. R.Sudha, P.Nivetha," A Novel Approach For Secure Data Transmission Using Cp_Abe And Md5 Algorithm In Wban", International Journal of Emerging Trends & Technology in Computer Science (IJETTCS) Volume 6, Issue 3, May- June 2017 ISSN 2278-6856


 

**Authors Profile**

***Ms.M.Infant Angel.***She is currently working as assistant professor in department of computer science,Park's College.Tirupur.She has published more than 3 research papers in reputed international journals and conferences it's also available in online.His main research work is focuses on wireless sensor networks.

***Dr.R.Sudha***.She is currently working as associate professor in department of computer science,psg college of arts & science,Coimbatore.She has published more than 15 research papers in reputed international journals, conferences, it's also available in online .His main research work focuses in Wireless sensor networks.She has 15 years of teaching experience and 9 years of research experience.

 