ISSN:2231-0711

Princy S et al | IJCSET(www.ijcset.net) | November 2015 | Vol 5, Issue 11,374-377

A Survey - Security Challenges and Schemes on Wireless Sensor Network

Princy S[#1], P.K. Sasikumar[*2]
[#1]*ME-Computer Science and Engineering*
Tamilnadu College Of Engineering, Coimbatore, India

[*2]*Assistant Professor*
Tamilnadu College Of Engineering,Coimbatore,India

***Abstract*—Wireless sensor network (WSN) is one of the emerging technologies to attract the researchers with its research challenges and can be applied on various domains. Now a day WSN applications are used on environmental detection, monitoring system, medical system, military and industrial is monitoring for transforming human life to different aspects. Depending on the applications used on the WSN, Security is one of the greatest challenges in WSNs and it is the essential part before designing the WSNs. In this paper a survey is taken related to the security on the wireless sensor network (WSN).**

***Keywords*—WSN, security, challenges, survey**

I. INTRODUCTION

Wireless sensor networks grow as one of the popular and widely used, but security becomes a greater serious concern. Users do not want for revealing the data by the unauthorized people as it disclosed information for the malicious purposes. These concerns are most relevant to the wireless environment in which anyone can overhead the message sent. Therefore for the convenient system may appeal to the users if it is not secure. To address these conflicts, researches in WSN have been implemented serval Security protocols needs to be used on the sensor network. Examples of such protocols are TinySec [1] and TinyECC [2].

In general security is considered to be more expensive. Its cost more in WSNs because of the limited resources in the sensor nodes. Thus in need to provide a sufficient level to security. Meanwhile it should be properly utilizing by the available resources. For Example [3] if a sensor device hasn't avail with the enough memory to run the particular algorithm that requires on the lessor memory but that may also be less secure.

There are more way to secure in WSNs than by using just an encryption algorithms. Modes of operation introduced to ensure the encrypting plaintext with the same key multiple times and could deliver the different cipher text.

Message Authentication Code (MAC) algorithm is used for providing guarantee to the authentication and integrity of data. We conform that all three- encryption algorithm, operation modes and MAC algorithms are mainly takes part on the security in WSNs as shown in fig 1. [8][10][12]. The data encryption algorithms used in WSNs are commonly divided as three types: Symmetric key algorithm, asymmetric key algorithm and hash algorithms. [3-6]

Fig 1 Data packet structure

II. LITERATURE REVIEW

In survey papers [5], [6], the symmetric key and hash based algorithm techniques are processed on WSNs. In these algorithms, every symmetric authentication key are to be share by the cluster on the sensor nodes. An intruder comprises the key with the capture on the single sensor node. Therefore these techniques are not adapted to the node compromise attacks. A secret polynomial depends message authentication techniques were discussed on [7]. This method presents the information on the theoretic security with the ideas on the threshold secret sharing, in which the threshold is calculated by the degree in the polynomial. While the number of messages transformed as the lower threshold the techniques applies the intermediate nodes to authenticity the message through the polynomial evaluation.

Wherever the number of messages transmitted is larger than the threshold, the polynomial must fully improve and thereby the system will completely damage. To boost up the threshold and the complexity among the intruder for reconstruction the secret polynomial, a random noise which is also called as perturbation factor, was developed to the polynomial in [8] from counting the coefficient of the polynomial.

Hence the added perturbation factor can entirely erased by using error correcting code schemes [13]. By using the public key based ap techniques, messages are transmitted through the sender private key together with the digital signature of the message given. The upgraded development on elliptic curve cryptography (ECC) depends on the term public key schemes which are more benefit on the memory usage; message complexity and security because public key based techniques have a simple and neat key management [15].

Wireless sensor network leads on the traditional networks in many ways like as large scale, autonomous nature and intense deployment [1] [14]. It also improves the fault tolerance since a sensor node fails others can gather the

data. Hence it develops more attractive on the particular application likewise syndrome surveillance, military, environmental observation, fire detection, supply chain management, energy automation, vision enabling, gaming, building administration, health and other commercial and home applications [15-28]

Thereby the extensive deployments of WSN used on the multi-faceted applications security are developing concern. For example on a battle ground, a military communication network applied to susceptible information exchange may be hacked on adversaries because of the WSN's security hole leads to stern loss of the life and machineries. Thus security of WSN is the greatest task because of its limited resources likewise power supplies, energy, computation, small memory and communication capability [29][30][31][14][33].Cryptographic algorithm plays a major role in the security and resource conservation of the wireless sensor network (WSN) [33] [34].

OVERVIEW ON WIRELESS SENSOR NETWORKS

Wireless Sensor Networks (WSN) is an interconnection to the large number of nodes that are deployed to monitor the system which means the measurement to its parameters. Recent research on wireless sensor networks that led for various new protocols that based particularly on the designed sensor networks. To design these networks, the factor needs to be considered under the coverage area, mobility, power consumption, communication capabilities etc. Wireless Sensor Architecture is shown and described below in the fig 2.

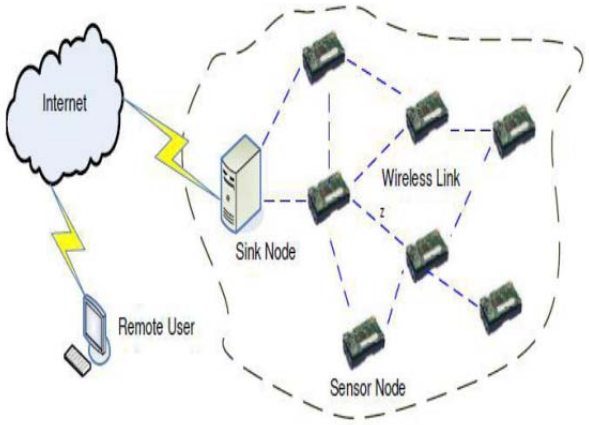

Fig-2. Wireless sensor network architecture

A. Characteristics of a WSN include:

- Power consumption constraints for nodes using batteries or energy harvesting
- Ability to cope with node failures
- Mobility of nodes
- Heterogeneity of nodes
- Scalability to large scale of deployment
- Ability to withstand harsh environmental conditions
- Ease of use
- Cross-layer design

B. Summary of various Security Schemes for Wireless Sensor Networks

Security Schemes	Attacks	Deterred Network Architecture	Major Features
JAM [38]	DoS Attack (Jamming)	Traditional wireless sensor network	Avoidance of jammed region by using coalesced neighbor nodes
Wormhole based [39]	DoS Attack (Jamming)	Hybrid (mainly wireless partly wired) sensor network	Uses wormholes to avoid jamming
Statistical En-Route Filtering [33]	Information Spoofing	Large number of sensors, highly dense wireless sensor network	Detects and drops false reports during forwarding process
Radio Resource Testing, Random Key Pre-distribution etc. [24]	Sybil Attack	Traditional wireless sensor network	Uses radio resource, Random key pre-distribution, Registration procedure, Position verification and Code attestation for detecting sybil entity
Bidirectional Verification, Multi-path multi-base station routing [40]	Hello Flood Attack	Traditional wireless sensor network	Adopts probabilistic secret sharing, Uses bidirectional verification and multi-path multi-base station routing
On Communication Security [32]	Information or Data Spoofing	Traditional wireless sensor network	Efficient resource management, Protects the network even if part of the network is compromised
TIK [27]	Wormhole Attack, Information or Data Spoofing	Traditional wireless sensor network	Based on symmetric cryptography, Requires accurate time synchronization between all communicating parties, implements temporal leashes
Random Key Predistribution [29], [30],[41]	Data and information spoofing, Attacks in information in Transit	Traditional wireless sensor network	Provide resilience of the network, Protect the network even if part of the network is compromised, Provide authentication measures for sensor nodes

Security Schemes	Attacks	Deterred Network Architecture	Major Features
[42]	Data and Information Spoofing	Distributed Sensor Network, Large-scale wireless sensor network with dynamic nature	Suitable for large wireless sensor networks which allows addition and deletion of sensors, Resilient to sensor node capture
REWARD [43]	Blackhole attacks	Traditional wireless sensor network	Uses geographic routing, Takes advantage of the broadcast inter-radio behavior to watch neighbor transmissions and detect blackhole attacks
TinySec [35]	Data and Information spoofing, Message Replay Attack	Traditional wireless sensor network	Focuses on providing message authenticity, integrity and confidentiality, Works in the link layer SNEP & μ
TESLA [6]	Data and Information Spoofing, Message Replay Attacks	Traditional wireless sensor network	Semantic security, Data authentication, Replay protection, Weak freshness, Low communication overhead.

III. CONCLUSION

This paper discusses about the security challenges and schemes in Wireless Sensor Network (WSN). Many among the attackers are against the security in Wireless sensor networks which are caused due to the insertion of fake information on the compromised nodes within the network. According to the false information on the compromised node, a mean is needs for detecting false reports. Thus the security schemes would help us for secure transmit of data among the sensor nodes.

REFERENCES

[1] Jian Li Yun Li Jian Ren Jie Wu, ―Hop-by-Hop Message Authentication and Source Privacy in Wireless Sensor Networks‖, IEEE Transactions On Parallel And Distributed Systems, pp 1-10, 2013

[2] Sadaqat Ur Rehman, Muhammad Bilal, Basharat Ahmad, Khawaja Muhammad Yahya, Anees Ullah, Obaid Ur Rehman, ―Comparison Based Analysis of Different Cryptographic and Encryption Techniques Using Message Authentication Code (MAC) in Wireless Sensor Networks (WSN)‖, IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 1, No 2, January 2012, pp 96-101

[3] Raymond Sbrusch, ―Authenticated Messaging In Wireless Sensor Networks Used For Surveillance‖, Thesis, The University Of Houston-Clear Lake, May, 2008

[4] Harsh Kumar Verma, Ravindra Kumar Singh, ―Performance Analysis of RC6, Twofish and Rijndael Block Cipher Algorithms‖, International Journal of Computer Applications (0975 – 8887) Volume 42– No.16, March 2012, pp 1-7

[5] F. Ye, H. Lou, S. Lu, and L. Zhang, ―Statistical en-route filtering of injected false data in sensor networks,‖ in IEEE INFOCOM, March 2004.

[6] S. Zhu, S. Setia, S. Jajodia, and P. Ning, ―An interleaved hop-by-hop authentication scheme for filtering false data in sensor networks,‖ in IEEE Symposium on Security and Privacy, 2004.

[7] C. Blundo, A. De Santis, A. Herzberg, S. Kutten, U. Vaccaro, and M. Yung, ―Perfectly-secure key distribution for dynamic conferences,‖ in Advances in Cryptology - Crypto'92, ser. Lecture Notes in Computer Science Volume 740, 1992, pp. 471–486

[8] W. Zhang, N. Subramanian, and G. Wang, ―Lightweight and compromise resilient message authentication in sensor networks,‖ in IEEE INFOCOM, Phoenix, AZ., April 15-17 2008.

[9] A. Perrig, R. Canetti, J. Tygar, and D. Song, ―Efficient authentication and signing of multicast streams over lossy channels,‖ in IEEE Symposium on Security and Privacy, May 2000.

[10] R. Rivest, A. Shamir, and L. Adleman, ―A method for obtaining digital signatures and public-key cryptosystems,‖ Communications. of the Assoc. of Comp. Mach., vol. 21, no. 2, pp. 120–126, 1978.

[11] T. A. ElGamal, ―A public-key cryptosystem and a signature scheme based on discrete logarithms,‖ IEEE Transactions on Information Theory, vol. 31, no. 4, pp. 469–472, 1985.

[12] M. Albrecht, C. Gentry, S. Halevi, and J. Katz, ―Attacking cryptographic schemes based on ―perturbation polynomials‖,‖ Cryptology ePrint Archive, Report 2009/098, 2009, http://eprint.iacr.org/.

[13] H. Wang, S. Sheng, C. Tan, and Q. Li, ―Comparing symmetric-key and public-key based security schemes in sensor networks: A case study of user access control,‖ in IEEE ICDCS, Beijing, China, 2008, pp. 11–18.

[14] Matthew N. Vella, Texas A&M University-Corpus Christi, Computer Science Program, Dr. Ahmed Mahdy Texas A&M University-Corpus Christi, Computer Science Faculty ―Survey of Wireless Sensor Network Security‖.

[15] Chung-Kuo Chang, J. Marc Overhage, Jeffrey Huang ―An Application of Sensor Networks for Syndromic Surveillance‖ 2005 IEEE

[16] Dunfan Ye,DaoliGong,WeiWang ―Application of Wireless Sensor Networks in Environmental Monitoring‖, 2009 2nd International Conference on Power Electronics and Intelligent Transportation System.

[17] Ling Tan, Shunyi Zhang, and Yanfeng Sun, Jing Qi ―Application of Wireless Sensor Networks in Energy Automation‖, Sustainable Power Generation and Supply, 2009. Supergen '09. International conference

[18] Sundip Misra, Vivek Tiwari and Mohammad S. Obaidat, Fellow, IEEE ―LACAS: Learning Automata-Based Congestion Avoidance Scheme for Healthcare Wireless Sensor Networks‖, IEEE Journal on Selected Areas in Communications, Vol. 27, No. 4, May 2009

[19] Ian F. Akylidiz, Fellow IEEE, Tommaso Melodia, Member IEEE, and Kaushik R. Chowdhury, Student Member IEEE ―Wireless Multimedia Sensor Networks: Applications and Testbeds‖, Proceedings of the IEEE. Vol. 96, No. 10, October 2008

[20] Kwangsoo Kim, Jongarm Jun, Sunjoong Kim, and Byung Y. Sung ―Medical Asset Tracking Application in Wireless Sensor Networks‖, The Second International Conference on Sensor Technologies and Applications, 2008 IEEE

[21] N. Rajendran, P. Kamal, D. Nayak, and S. A. Rabara, ―WATSSN: A Wireless Asset Tracking System using Sensor Networks‖, Proceedings of IEEE International Conference On Personal Wireless Communications, Jan 2005

[22] G. W. Allen, K. Lorinca, M. Welsh, O. Marcillo, J. Johnson, M. Ruiz, and J. Lees, ―Deploying a Wireless Sensor Network on an Active Volcano‖, IEEE Internet Computing, IEEE Computer society, March/April 2006

[23] K. Chintalapudi, T. Fu, J. Paek, N. Kothari, S. Rangwala, J.Caffrey, R. Govindan, E. Johnson, ―Monitoring Civil Structures with a Wireless Sensor Network‖, IEEE Internet Computing, IEEE Computer society, March/April 2006

[24] I. Ituen and G. Sohn, ―The Environmental Applications of Wireless Sensor Networks‖, International Journal of Contents, Vol.3, No. 4, Dec 2007
[25] A. Mainwaring, J. Polastre, R. Szewczyk, D. Culler, J. Anderson, ―Wireless Sensor Networks for Habitat Monitoring‖, WSNA'02, Sep 2002
[26] Anthony Rowe, Dhiraj Goel, Raj Rajkumar ―FireFly Mosaic: A Vision-Enabled Wireless Sensor Networking System‖, 28th IEEE International Real-Time Systems Symposium. 2007 IEEE
[27] E. Sazonov, K. Janoyan, and R. Jha, ―Wireless Intelligent Sensor Network for Autonomous Structural Health Monitoring‖, Proceedings of Structural Materials Technology (SMT): NDE/NDT for Highways and Bridges, 2004
[28] http://corporate.traffic.com
[29] Xiaojiang Du, North Dakota State University and Hsiao-Hwa Chen, National Cheng Kung University ―Security in Wireless Sensor Networks‖ IEEE Wireless Communication August 2008
[30] Sung-Chul Jung , Hyoung-Kee Choi. School of Information and Communication Engineering ―An Energy-aware Routing Protocol Considering Link-Layer Security in Wireless Sensor Networks.‖ Feb.15-18, 2009 ICACT 2009
[31] Md. Anisur Rahman and Mitu Kumar Debnath ―An Energy-Efficient Data Security System for Wireless Sensor Network‖ Proceedings of 11th International Conference on Computer and Information Technology (ICCIT 2008) 25-27 December, 2008, Khulna, Bangladesh
[32] Al-Sakib Khan Pathan, Hyung-Woo Lee, Choong Seon Hong ―Security in Wireless Sensor Networks: Issues and Challenges‖ Feb. 20-22, 2006 ICACT 2006
[33] Mohammad AL-Rousan, A.Rjoub and Ahmad Baset ―A lowenergy security algorithm for exchanging information in wireless sensor networks‖, Journal of information assurance and security 4 (2009) 48-59.
[34] Y.W. Law, S. Dulman, S. Etalle, P. Havinga (2002), ―Assessing security critical energy efficient sensor network‖, Available at: http://www.dsv.su.se/~matei/bin/4%20- %202i1279/L5_EYES.pdf
[35] Pister, K., "29 Palms fixed/mobile experiment: Tracking vehicles with a UAV delivered sensor network," 2001.
[36] Bishop, M., Computer security: art and science. Boston, MA: Addison-Wesley, 2003
[37] Schneier, B., Applied cryptography : protocols, algorithms, and source code in C, 2nd ed. New York: Wiley, 1996.
[38] Wood, A. D. and Stankovic, J. A., "Denial of service in sensor networks," IEEE Computer, vol. 35, pp. 54-62, 2002.
[39] Wood, A. D., Fang, L., Stankovic, J. A., and He, T., "SIGF: a family of configurable, secure routing protocols for wireless sensor networks," Proceedings of the fourth ACM workshop on Security of ad hoc and sensor networks, pp. 35-48, 2006.
[40] Wang, X. and Yu, H., "How to Break MD5 and Other Hash Functions," Advances in Cryptology – EUROCRYPT 2005, pp. 19-35, 2005.
[41] Rivest, R., "The MD5 Message-Digest Algorithm, RFC 1321," IETF, 1992.