I J C T A, 9(34) 2016, pp. 361-366

Efficient Key Management for Security in Wireless Sensor Network: A Survey

Niraj Nirmal*, Manish K. Ahirwar* and Anjana Deen*

ABSTRACT

Wireless sensor networks (WSNs) are used in wide areas.These networks belongs to infrastructureless class of network. In infrastructureless networks communication is done via wireless medium and security becomes a major aspect of these networks. In wireless mode of communication messages are generally encrypted so that only legitimate users can access the message. Many cryptography algorithms are proposed for wireless sensor networks, but the performance relays on key management and distribution approach used. In this paper a survey is done on key management and distribution for wireless networks.

Keywords: Wireless sensor networks, key management, asymmetric key distribution.

INTRODUCTION

Wireless Sensor Network (WSN) [8] is the network that consists of many small devices that called sensors. WSN belongs to the class of ad hoc networks as these are also infrastructure less networks [1,3]. These networks are very useful in daily life; they find applications in military, healthcare, and in environmental areas. Hence, the communications in these types of networks need to be secure due to their use in sensitive areas. To provide the Security for the communication in WSN is an important issue, due to the ad - hoc nature of WSN. Links for the communication in these types of networks are radio links, but the radio links are easily vulnerable to various types of attacks such as malicious attacks. There are several limitations of Sensors devices in resources can control the nature and working for WSNs which is also affecting the security level for this type of networks. WSN has following limitations like battery age, less memory space, processing power, random distribution of nodes, transmission range and bandwidth [2].

Since the WSN has such constraints, and is vulnerable to attackers, security in WSN is a great challenge. Many algorithms have been proposed in the literature to achieve this task. In fig. 1 CA is Certificate Authority, which provides a key to all nodes in the cluster.

WSN needs a cryptography algorithm [18,15] that must be selected carefully, and the most important factor is key management and distribution. A secure channel is required for communication between sensor nodes.

The cryptographic algorithm has to meet principles of security which includes confidentiality, integrity, authenticity, and availability (CIAA) [5]. Confidentiality ensures secrecy of the exchanged data between nodes, and could not be detected by non deliberate nodes. Therefore, key establishment and distribution mechanism will be effective when the generated keys are secure and data which are exchanged or communicated will be secured [2]. Integrity represents that any type of alteration or modification of the data cannot be done without a legitimate node. Availability means to have 24X7 operation of network for users. In WSN the most frequent attack is a denial of service. The various constraints on WSN resources

* Dept. of CSE, University Institute of Technology, RGPV, Bhopal , India, *E-mails: nnirmaly@gmail.com; Ahirwarmanish@gmail.com; anjnadeen@yahoo.com*

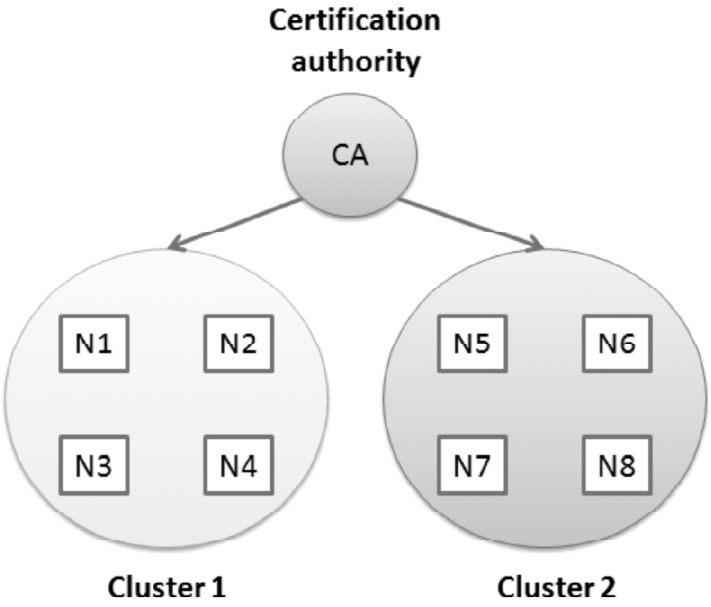

Figure 1: Figure showing wireless network of 2 clusters with CA

have a huge effect on the availability requirement. The battery duration for sensor nodes is limited and may discharge it and its a cause of an interruption in the service and may violate availability. So, key establishment technique and security algorithms should take care of these limitations. In security, the authentication ensures identity of the nodes in WSN. The key management mechanism [16] should not allow for any strange node to participate in any communication process that takes place in the WSN.

PRINCIPLES OF SECURITY

For every secure network all the principles of security must be considered for reliable and continuous operation of network. Following are the principles of security:

- Authentication.
- Authorization.
- Integrity.
- Confidentiality
- Non repudiation.

Kerberos and other schemes to verify identity of the user are used for authentication. And to check user privileges authorization is done. Cryptography is used for confidentiality and privacy concern. Digital signature and some certificate less schemes are used for protection from non repudiation.

LITERATURE REVIEW

M. Rahman *et al.* [2] discussed a private key agreement for secure communication in wireless sensor network. The challenges of secure sensor routing are discussed, together with security threat and counter-measurement analysis on a few popular routing protocols. However, it does not consider the fabricated data injection attacks launched by compromised nodes.

M. R. Alagheband *et al.* [3] discussed key management hierarchy based for wireless sensor network. To reduce overhead of centralized key distribution authority hierarchical scheme is used.

Two recent studies of SEF [13] and Hop-by-Hop Authentication [14] address the problem of selecting secure path to transmit the data in WSN. Unwanted traffic forwarding and heavy security algorithms may

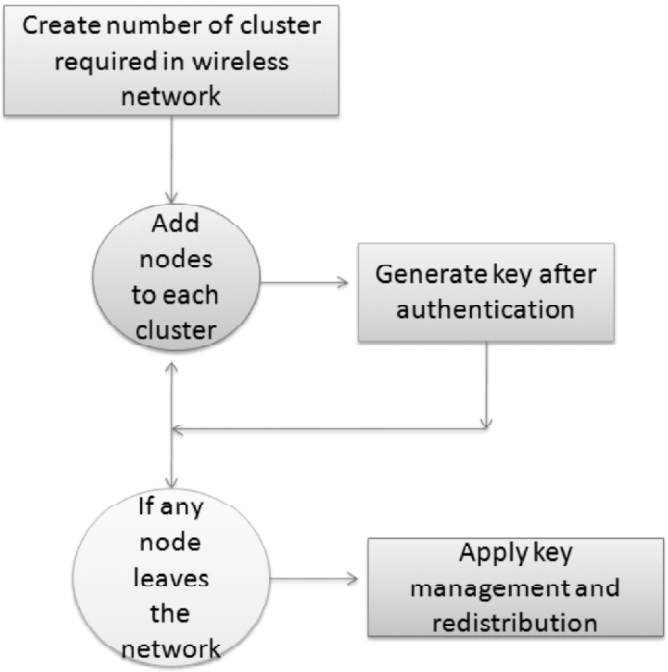

Figure 2: Showing key management in wireless networks

also result in draining out battery life of nodes. Secure Diffusion [14]follows different approach that handles the malicious traffic through implicit rate control [13] and negative reinforcement mechanisms. As a result, Secure Diffusion is resilient to an increasing number of compromised nodes, whereas both SEF and Hop-by-Hop Authentication completely lose security protection when the attacker has compromised beyond a small, fixed number of nodes.

Key management is a critical and challenging task in WSNs. In [8, 16, 17] a number of paired symmetric key establishment schemes have been proposed by respective authors. Probabilistic key sharing [14] is used widely to establish trust between two nodes with different emphasis on enhanced security protection [11], high probability of key establishment and reduced overhead [15],flexibility of security requirements [17], or utilization of deployment knowledge [12]. Such paired keys are used to authenticate node's identity or messages; how- ever, false generatedsensing data for wasting battery life by compromised nodes cannot be handled. Instead, semantic verification of the data is required to detect the fabricated ones. Secure Diffusion exploits location-based key management to achieve this goal. Because the data authentication keys are bound to geographic locations, the compromised nodes outside the targeted region, no matter how many there are, cannot fabricate sensing data without being detected. Secure routing has been extensively studied in the context of ad-hoc networks [9, 10, 11]. However, none of these protocols can be applied in sensor networks, because none addresses the unique feature of data-centric communication, and the network scale is limited by the excessive number of keys each node should store.

I.-H. Chuang et al. [5] proposed a clustering based key management algorithm for wireless sensor network.

W. T. Zhu et al. [17] discussed node replication attack for wireless sensor network. Spoofing and identity theft are discussed.

M. A. Rassam et al. [18] done survey on intrusion detection techniques and attacks on wireless sensor networks. Some other schemes and key management and redistribution schemes are discussed in tables shown below.

B. Butani et al. [19] has done surveys on node capture attack in WSN and also analyzed various types of detection and key- pre-distribution for efficient to resilience against node capture attack.

DeshrajAhirwar et al. [20] surveyed network security enhancement techniques. AnkurKhare et al. [21] implemented a fast chaotic encryption scheme using digital logic circuits for adhoc networks.Piyush Kumar Shukla et al. [23] discussed architecture, design and security issues in wireless sensor networks. Parvez Khan et al. [24] discussed capacitryenchancement in wireless sensor networks using multi hop routing protocols. Piyush Kumar Shukla et al. [25] discusses a Robust Assailant Using Optimization Functions (FiRAO-PG) in Wireless Sensor Network.

Table 1 (Comparison Table)

Features	*W. Du, J. Deng et al. [1]*	*M. Rahman et al. [2]*	*M. R. Alagheband et al. [3]*	*D. S. Sanchez et al. [4]*	*I.-H. Chuang et al. [5]*	*S. Agrawal et al. [6]*
Type of key distribution	Asymmetric	Asymmetric	Asymmetric	Asymmetric	Symmetric	Symmetric
Key distribution scheme	Pair wise pre-distribution scheme	Private key agreement	Hierarchical key management	Pairwise key distribution	Two layered dynamic key management	Novel key updating
Authentication	Private key authentication	Private key authentication	Private key authentication	Private key authentication	Single key authentication	Single key authentication
Cryptographic algorithm used	RSA	Diffie-Hellman	RSA	Elliptic curve Cryptography	NA	NA
Digital signature	Yes	Yes	Yes	Yes	NO	NO

Table 1 Conti.

Features	*S. U. Khan et al. [7]*	*X. Zhang et al. [8]*	*S. S. Al-Riyami et al. [10]*	*S. SEO et al. [11]*	*X.-J. Lin et al. [14]*	*P. Szczechowiak et al. [15]*
Type of key distribution	Asymmetric	Asymmetric	Asymmetric	Asymmetric	Asymmetric	Asymmetric
Key distribution scheme	Energy efficient key distribution scheme	Energy efficient key distribution scheme	Certificate-less public key scheme	Pairwise key distribution	Hierarchical key management	Hierarchical key management
Authentication	Private key authentication	Private key authentication	Certificate-less authentication	Pair key authentication	Private key authentication	Private key authentication
Cryptographic algorithm used	RSA	Diffie-Hellman	NA	Elliptic curve Cryptography	NA	Nano ECC
Digital signature	Yes	Yes	Certificate-less approach	Certificate-less approach	YES	YES

Table 2 (Techniques used in Key Management)

Technique	*Description*	*Advantages*	*Disadvantages*
Symmetric key distribution scheme	In this kind of approach single key is distributed among those whom we intend to share private data. A single key is used to encrypt and decrypt the data in a network.	Faster, Low Computation, Only One Secret Key Required, Less memory required.	Key exchange, Low security,
Asymmetric key distribution scheme	In these techniques public-private key pair is distributed among the nodes. And private key is used to encrypt the data while the public is used to decrypt.	Provide message authentication, more secure, no need to exchangekeys	Slow, More computational, Required large memory
Key distribution schemes	In large wireless sensor networks key distribution and management is a challenging task. Many key distribution schemes are proposed by various authors.	Distribution of public keys is easier	Distribution of the secret key is tough

contd. table

Technique	*Description*	*Advantages*	*Disadvantages*
Hop based authentication	In such networks every hop plays a role in security and authentication of WSN.	Compromised node identification, efficient wormhole detection	Don't detect the black hole attack
Elliptic curve cryptography and digital signature	ECC and digital signatures are used for key generation and non-repudiation avoidance in WSNs.	Faster and requires less computing power	More complex and more difficult to implement than RSA
Energy and memory efficient key updation	Key updation and redistribution also imparts considerable overhead to the security scheme used. Some of the schemes are discussed in the paper.	Better Security, Low Complexity	Key Overhead

SUMMARY

In this Survey paper key management methods in WSN for security i.e. authenticity, authorization, confidentiality, integrity and non- repudiation are discussed**.** For security in WSN, In past,Symmetric key distribution scheme used but due to high computational overhead and problem in key exchange it is not more secure and efficient. After that Public key Cryptography algorithms such as RSA, ECC with DSA etc. comes in use which is more scalable, flexible and resilient to node compromised than Symmetric key Cryptography algorithms. For more efficient and better security of nodes in WSN, key management schemes comes in role and for that key distribution scheme, whichdistributes the key to all the nodes for communicate each other without node impersonation, node compromiseand also physical attackof nodes. In this scheme every node has a key with certificate for encrypt as welldecryptthe messages which is passing over wireless medium as a radio signal. If any node leaves or joins the cluster again key distribution process is done and for this reason certificate is required every time which causes certificate overhead. To remove this drawback there certificate less Public key cryptography (CL-PKC) is used which is more energy efficient key updation.

CONCLUSION

In this paper a survey is done on key management approaches for wireless sensor networks. It is found that security approach must include all 5 security parameters that is authenticity, authorization, confidentiality, integrity and non- repudiation.

REFERENCES

[1] W. Du, J. Deng, Y. S. Han, P. Varshney, J. Katz, and A. Khalili,"A pairwise key predistribution scheme for wireless sensor networks", ACM Tran. Info. Syst. Secu., vol. 8, no. 2, pp. 228–258, 2005.

[2] M. Rahman and K. El-Khatib,"Private key agreement and secure communication for heterogeneous sensor networks", J. Parallel Dist. Comput., vol. 70, no. 8, pp. 858–870, 2010.

[3] M. R. Alagheband and M. R. Aref,"Dynamic and secure key management model for hierarchical heterogeneous sensor networks", IET Infor. Secu., vol. 6, no. 4, pp. 271–280, Dec. 2012.

[4] D. S. Sanchez and H. Baldus,"A deterministic pairwise key predistribution scheme for mobile sensor networks", in Proc. 1st Intr. Confer. Secu. Comm., pp. 277–288, Sep. 2005.

[5] I. H. Chuang, W.T.Su, C. Y. Wu, J.-P.Hsu, and Y. H. Kuo,"Two layered dynamic key management in mobile and long-lived cluster based wireless sensor networks", in Proc. IEEE WCNC, pp. 4145–4150, Mar. 2007.

[6] S. Agrawal, R. Roman, M. L. Das, A. Mathuria, and J. Lopez,"A novel key update protocol in mobile sensor networks", in Proc. 8th Inter. Confer. ICISS, vol. 7671, pp. 194–207, 2012.

[7] S. U. Khan, C. Pastrone, L. Lavagno, and M. A. Spirito, "An energy and memory-efficient key management scheme for mobile heterogeneous sensor networks", in Proc. 6th Inter. Confer. CRiSIS, pp. 1–8, Sep. 2011.

[8] X. Zhang, J. He, and Q. Wei, "EDDK: Energy-efficient distributed deterministic key management for wireless sensor networks", EURASIP J. Wireless Commun. Netw., vol. 2011, pp. 1–11, Jan. 2011.

[9] N. Gura, A. Patel, A. Wander, H. Eberle, and S. C. Shantz,"Comparing elliptic curve cryptography and RSA on 8-bit CPUs", in Proc. 6th Inter. Workshop Crypto. Hardw.Emb.Syst., pp. 119–132, 2004.

[10] S. S. Al-Riyami and K. G. Paterson,"Certificateless public key cryptography", in Proc. 9th Inter. Confer. ASIACRYPT, vol. 2894., pp. 452–473, 2013.

[11] S. Seo and E. Bertino,"Elliptic curve cryptography based certificateless hybrid signcryption scheme without pairing", CERIAS, West Lafayette, IN, USA, Techn. Rep. CERIAS TR 2013-10, 2013.

[12] S. H. Seo, J. Won, and E. Bertino,"POSTER: A pairing-free certificateless hybrid sign-cryption scheme for advanced metering infrastructures", in Proc. 4th ACM CODASPY, pp. 143–146, 2014.

[13] Q. Huang, J. Cukier, H. Kobayashi, B. Liu, and J. Zhang,"Fast authenticated key establishment protocols for self-organizing sensor networks", in Proc. 2nd ACM Inter. Confer. WSNA, pp. 141–150, 2003.

[14] X.-J. Lin and L. Sun,"Cryptanalysis and improvement of a dynamic and secure key management model for hierarchical heterogeneous sensor networks", in Proc. IACR Cryptol. ePrint Arch., pp. 698–698, 2013.

[15] P. Szczechowiak, L. B. Oliveira, M. Scott, M. Collier, and R. Dahab,"NanoECC: Testing the limits of elliptic curve cryptography in sensor networks", in Proc. 5th Euro. Confer. WSN, vol. 4913, pp. 305–320, 2008.

[16] K. Chatterjee, A. De, and D. Gupta,"An improved ID-based key management scheme in wireless sensor network", in Proc. 3rd Inter. Confer. ICSI, vol. 7332, pp. 351–359, 2012.

[17] W. T. Zhu, J. Zhou, R. H. Deng, and F. Bao,"Detecting node replication attacks in mobile sensor networks: Theory and approaches", Secu. Commu.Netw., vol. 5, pp. 496–507, 2012.

[18] M. A. Rassam, M. A. Maarof, and A. Zainal,"A survey of intrusion detection schemes in wireless sensor networks", Ameri. Jour. Appl. Scie., vol. 9, no. 10, pp. 1636–1652, 2012.

[19] B. Butani, P. K. Shukla and S. Silakari,"Optimized and Executive Surve of Physical Node Capture Attack in Wireless Sensor Network", in IJCNIS Vol. 6, No. 11, October 2014.

[20] DeshrajAhirwar, Manish K. Ahirwar, Piyush K. Shuklaand PankajRichharia "An analytical survey on Network SecurityEnhancement Services" in *(IJCSIS) International Journal of Computer Science and Information Security,Vol. 9, No. 3, March 2011*.

[21] Ankur Khare, Piyush Kumar Shukla, Murtaza Abbas Rizvi and Shalini Stalin "An Intelligent and Fast Chaotic Encryption Using Digital Logic Circuits for Ad-Hoc and Ubiquitous Computing" in Entropy **2016**, 18, 201; doi:10.3390/e18050201.

[22] Piyush Kumar Shukla, Kirti Raj Bhatele, Lokesh Sharma, Poonam Sharma and PrashantShukla "Design, Architecture,and Security Issues inWireless Sensor Networks" in A volume in the Advances inInformation Security, Privacy,and Ethics (AISPE) Book Series.

[23] Parvez Khan, AnjanaJayantDeen, Manish Ahirwar "Enhance wireless Capacity through Multi-hop Scheduling" in International Journal of Scientific & Engineering Research, Volume 5, Issue 10, October-2014.

[24] Piyush Kumar Shukla, SachinGoyal, Rajesh Wadhvani, M. A. Rizvi, PoonamSharma andNeerajTantubay "Finding Robust Assailant Using Optimization Functions (FiRAO-PG) in Wireless Sensor Network".