Journal of Computer Science 7 (6): 849-853, 2011
ISSN 1549-3636

Authenticated Broadcast in Heterogeneous Wireless Sensor Networks using Chinese Remainder Theorem Algorithm

[1]Kalyani Palanisamy and [2]Chellappan
[1]Department of Computer science and Engineering, I.R.T.T., Erode, India
[2]Department of Computer Science and Engineering,
Anna University Chennai, India

Abstract: Problem statement: The security in Wireless Sensor Networks (WSN) is a critical issue due to the inherent limitations of computational capacity, storage capacity and power usage. Key management only makes sure the communicating nodes possess the necessary keys, at the same time protecting the confidentiality, integrity and authenticity of the communicated data. **Approach:** Proposed a RSA-CRT methodology for authenticated broadcast in the wireless sensor networks and analyzed the proposed with existing methodologies indicating their advantages, drawbacks and weaknesses. **Results:** The proposed RSA with CRT algorithm is improved the secured routing paradigm and provides efficient key management which using optimal encryption/decryption of broadcast messages authentication. **Conclusion:** The proposed system countermeasures the attacks in the network layer of WSN and it will reduce the communication overhead, storage space and energy consumption of nodes.

Key words: Wireless Sensor Networks (WSN's), security issues, key management, Chinese Remainder Theorem (CRT), authenticated broadcast, asymmetric keys algorithms, control domain, Public Key Encryption (PKE), cluster keys, node keys

INTRODUCTION

Wireless Sensor Networks (WSN's) are quite useful in many applications since they provide a cost effective solution to many real life problems. But it appears that they are more prone to attacks than wired networks .They are susceptible to a variety of attacks, including node capture, physical tampering and denial of service, prompting a range of fundamental research challenges (Perrig *et al*., 2004), an attacker can easily eavesdrop on, inject or alter the data transmitted between sensor nodes. Security allows WSNs to be used with confidence and maintains integrity of data. Providing security in wireless sensor networks is pivotal due to the fact that sensor nodes are inherently limited by resources such as power, bandwidth, computation and storage. A survey of security issues in adhoc and sensor networks and related work can be found Djenouri and Khelladi (2005) Gaubatz *et al*. (2004) Perrig *et al*. (2002). All approaches of security analysis in WSNs are scenario depended, e.g., An Agricultural application, a habitat monitoring and remote operations and control domain (Zurina, 2009; Sundararajan and Shanmugam, 2010; Mbaitiga, 2009). In the above all the operations are sensitive to possible attacks and they have not concentrated on the key management schemes which only gives solution to the reliable and secured communication in WSN. Key management only makes sure the communicating nodes possess the necessary keys, at the same time protecting the confidentiality, integrity and authenticity of the communicated data.

MATERIALS AND METHODS

Security mechanisms in WSN are developed in view of certain constraints and are classified into two types. One is security needed for operations and another is security for information. The objectives of these securities are, first the network should continue its function even when some of its components attacked which is shown in Table 1 and CIA of information should never be disclosed respectively.

The security in WSNs is critical issue due to the inherent hardware limitations and constraints: (1) Energy efficiency, (2) No public-key cryptography, (3) Physically tampers able, (4) Multiple layers of defense.

Security becomes an important concern because attacks can occur on different layers of a networking stack. Naturally it is evident that a multiple layer of defense is required, i.e., a separate defense for each layer (Yang *et al*., 2004).

Corresponding Author: Kalyani Palanisamy, Department of Computer science and Engineering, I.R.T.T., Erode, India

Table 1: Different types of attacks and mode of defense in Network layer of sensor network

	Main security concern	Available Modes of defence			
		Mode	Strength	Weakness	Best optional choice
Network layer	Hello-flooding				Authenticated Broadcast and Efficient key-management
	Neglect /discard				Multi path routing
	Black holes or sink hole	Key Management Schemes			REWARD algorithm
	Sybil	Radio-resource testing and random key predistribution			Key-management architecture
	Worm holes	TIK	Implements Temporal-leashes	Requires synchronization Computationally expensive	TIK based upon symmetric cryptography

Table 2: Comparison of symmetric and asymmetric keys

Symmetric	Asymmetric
Single key approach WSN need to store n-1 keys in sensor node for network size n. Complicated one way key chain	Two key approach one public, one private key. Also reduced key storage
Large computations required more energy	Less computation, so less energy
Need key distribution.	No need for key pre distribution. Since Secrete key is private, inverse calculation is not possible, so more secure.
Fixed key length	Variable key length provides data CIA and supports group key management
Complicated needs key sharing	no pair wise key sharing, More flexible and simple interface suitable for WSN

It is difficult to identify the suitable cryptography for WSNs because of its inherent limitations in terms of energy, computational power and storage capacity. Most previous schemes proposed for WSNs security have used symmetric cryptography (DES,AES,RC4)than asymmetric cryptography (RSA,ELGAMAL,ECC) as asymmetric keys are used for key generation (Delgosha, 2009). Table 2 summaries the advantages and disadvantages of a symmetric over symmetric keys.

In this study an effort made to analysis various asymmetric keys algorithms ELGAMAL, RSA (Rivest Shamir Adelman), Public Key Encryption (PKE), Elliptic Curve Cryptography (ECC) which are used for key distribution as well as encryption/decryption in sensor network for authenticated message broad cast. The analysis shows that RSA is better than ELGAMAL and PKE. But comparing ECC the effort needed for RSA is rather too much and so ECC is better than RSA for security in WSNs. We proposed a method to enhance and improve the performance of RSA by applying Chinese Remainder Theorem (CRT) in decryption phase of RSA. This concept of applying CRT in the decryption phase of RSA is utilized in Hardware fault attacks and shows better performance This concept has been tested in hardware like CPU, RAM, EPROM, Smart card processors fault attacks and shows improvement in speed and reduced computation time and space for the RSA cryptography algorithm (Xiao *et al*., 2007; Vigilant, 2008). The same concept of applying CRT in the decryption phase of RSA algorithm used for message authentication in WSN will give advantages over the methods studied (ELGAMAL,RSA,PKE) with respect to energy, computation time, storage space, speed of processing in turn reduces the communication over heads.

In the literature of WSN, Priority and Random Selection for Dynamic Window Secured Implicit techniques (Hanapi *et al*., 2009), Optimal Power Multicast (Maalla *et al*., 2009), Low Power Phase Locked Loop Frequency Synthesizer (Ismail and Othman, 2009), Transportation Infrastructural Health (Chang and Mehta, 2010), Ethical Issues in E-Commerce (Nardal and Sahin, 2011) are available resources for further studies.

RSA with CRT: RSA operations are modular exponentiations of large integers with a typical size of 512-2048 bits. RSA encryption generates a cipher text C from a message M based on a modular exponentiation $C = M^e \bmod n$. Decryption regenerates the message by computing $M = C^d \bmod n$[1]. Among the several techniques that can be used to accelerate RSA. This paper specifically focused on those applicable under the constraints of sensor nodes.

Chinese remainder theorem: RSA private-key operations, namely decryption and signature generation, can be accelerated using the Chinese Remainder Theorem (CRT). RSA chooses the modulus n as the

product of two primes p and q, where p and q are on the order of √n (e.g. for a 1024-bit n, p and q are on average 512 bits long). Using the CRT, a modular exponentiation for decryption $M = C_d \bmod n$ can be decomposed into two modular exponentiations $M_1 = C_1^{d1} \bmod p$ and $M_2 = C_2^{d2} \bmod q$, where C_1, d_1, C_2 and d_2 are roughly half the size of n. Assuming schoolbook multiplication with operands of size $m/2 = [\log_2 (n)]/2$, modular multiplications can be computed in roughly 1/4 of the time as m-bit modular multiplications. Thus the CRT reduces computation time through Montgomery multiplication by nearly 3/4 resulting in up to a 4x speedup.

Key management schemes: Key management is the process in which cryptographic keys are generated, stored, protected, transferred, loaded, used and destroyed. There are four principal concerns in a key management framework are given below:

- Key deployment/pre-distribution: Method to find the number of keys required and method to distribute the keys before the nodes are deployed
- Key establishment: Establish the secure session between any pair or group of sensor nodes or between node to cluster head and in turn to base station
- Member/node addition: Method for a node to be added to the network such that it be able to establish secure sessions with existing nodes in the network, while not being able to decipher past traffic in the network
- Member/node deletion: Method for a node to be evicted from the network such that it will not again be able to establish secure sessions with any of the existing nodes in the network and not be able to decipher future traffic in the network

The major advantages and drawbacks of different key distribution and management schemes are summarized in Table 3.

Key establishment: Establishment of keys in sensor networks can also be realized with protocols where the nodes set up a shared secret key after deployment, either through key transport or key agreement. The advantage of key agreement over key transport is that no entity can predetermine the resulting key as it depends on the input of all participants. There are three types of general key agreement schemes: 1.trusted-server schemes, 2.self-enforcing scheme and 3.key pre-distribution scheme. First the Trusted server scheme depends on trusted server for key agreement between nodes (e.g., Kerberos) is not suited for WSNs because there is no trusted infrastructure in WSNs. Second, Self enforcing scheme depends on asymmetric cryptography using public key algorithm for key agreement (Diffie-Hellman, RSA) which needs high computation capability and energy which limits its use. The third type is key pre-distribution scheme where all key are pre distributed to all sensor nodes prior to deployment. In our proposed method takes the advantages of the public key algorithm scheme and third key pre distribution scheme are combined together to achieve efficient key management scheme which will reduce the energy consumption and communication overheads even with limited resources.

Various Keys used in sensor network: There are various communication patterns in sensor networks. The following types of keys are used in WSNs.

Network key: A key that is shared by all nodes in the network and is used to encrypt and decrypt global messages. It cannot be used for message authentication:

- Cluster keys: A key shared by a cluster head node and its neighbor nodes to encrypt and decrypt local broadcast messages. It cannot be used for message authentication
- Link keys: A key shared by two neighbor nodes (two sensor nodes or sensor and base station) it provides protection for unicast messages between neighboring nodes. They can be used for encryption, message authentication and integrity protection. They can also be used to set up other keys between neighboring nodes (e.g., Cluster keys)
- Node keys: A key that is shared by sensor node and base station. It is used to protect unicast messages exchanged between the sensor node base stations that do not need in-networking processing

RESULTS AND DISCUSSION

The methodology is implemented in NS2. The performance analyses of the proposed methodology are given in the Table 3-5 and in the Fig. 1-4. The requirement of Storage Space in Mega-byte is shown in Table 3 and Fig. 1. Energy Consumption of each node in milli Watt is shown in Table 4 and Fig. 2. Time Consumption for Key Exchange in client and server side are shown in Table 5 and Fig. 3-4.

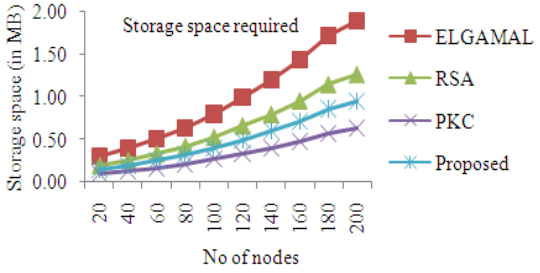

Fig. 1: Comparison of storage space requirement between (ELGAMAL, RSA, PKC) and proposed system

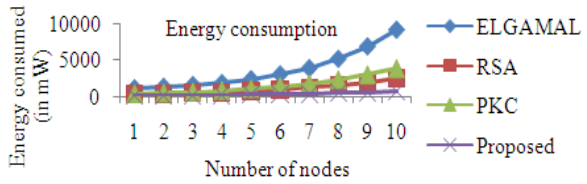

Fig. 2: Comparison of energy consumption between (ELGAMAL, RSA, and PKC) and proposed system

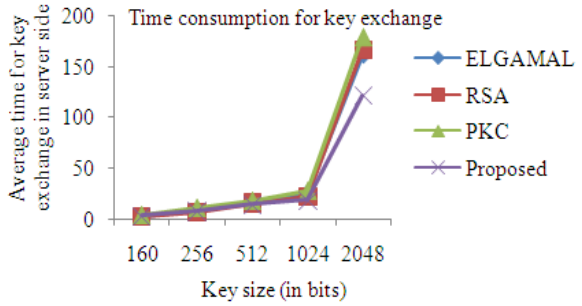

Fig. 3: Comparison of time consumption for key exchange in server side between (ELGAMAL, RSA, and PKC) and proposed system

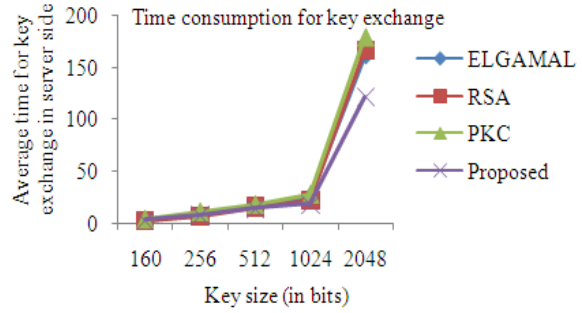

Fig. 4: Comparison of time consumption for key exchange in client side between (ELGAMAL, RSA, and PKC) and proposed system

Table 3: Storage Space Required (in MB)

No of Nodes	Elgamal	RSA	PKC	Proposed
20	0.30	0.20	0.10	0.15
40	0.39	0.26	0.13	0.20
60	0.51	0.34	0.17	0.25
80	0.63	0.42	0.21	0.32
100	0.79	0.53	0.26	0.40
120	0.99	0.66	0.33	0.50
140	1.19	0.79	0.40	0.59
160	1.43	0.95	0.48	0.71
180	1.71	1.14	0.57	0.86
200	1.88	1.25	0.63	0.94

Table 4: Energy consumption (in mW)

No of Nodes	Elgamal	RSA	PKC	Proposed
200	1120	273.8	412.3	102.7
400	1321.60	350.46	527.74	126.32
600	1559.49	448.59	675.51	155.37
800	1840.20	574.20	864.66	191.11
1000	2355.45	734.98	1106.76	235.07
1200	3014.98	940.77	1416.65	289.13
1400	3859.17	1204.19	1813.31	355.63
1600	5132.70	1541.36	2321.04	437.43
1800	6826.49	1972.94	2970.93	538.04
2000	9079.23	2525.36	3802.80	661.78

CONCLUSION

WSN security is very important issue motivated towards ensuring security under strict constraints. While analyzing the various attacks in the network layer of WSNs there are two issues multi path routing support and node specific key pre-distribution support are taken for consideration in this study. These are the two possible countermeasures identified for the attacks like Neglect, Hallo-flooding, Sybil attack in the network layer of WSNs and a new key management scheme need to be implemented. In this view we proposed a new efficient key management scheme RSA-CRT algorithm to support both multi path and node specific key pre-distribution for authentication of message broadcast in Wireless Sensor Networks(WSNs). The proposed method takes the advantages of the self enforcing scheme i.e., public key algorithm and key pre distribution scheme and are combined together to further improve the key management scheme which will reduce the energy consumption and communication overheads even with limited resources than a popular key management scheme for WSNs. Further, the proposed algorithm RSA-CRT enhances the performance of RSA which can be used for the encryption (RSA) and decryption (CRT) for authenticated message broadcast in wireless sensor networks along with key pre distribution. The proposed new algorithm implemented and simulated in NS2 simulator and the results shows that improvement in performance and reduced energy consumption and time delay thus increases the network life time and reduced communication over heads.

Table 5: Time consumption for key exchange in client and server side

	Time consumption for key exchange in server				Time consumption for key exchange in client			
Key size (in bits)	ELGAMAL	RSA	PKC	Proposed	ELGAMAL	RSA	PKC	Proposed
160	3	3	4	3	1.32	1.23	1.78	1.11
256	9	7	11	8	4.80	4.30	5.20	4.06
512	17	16	18	15	8.28	7.37	8.62	7.01
1024	26	22	28	19	11.76	10.44	12.04	9.96
2048	161	166	178	122	15.24	13.51	15.46	12.91

REFERENCES

Chang, C. and R. Mehta, 2010. Fiber optic sensors for transportation infrastructural health monitoring. Am. J. Eng. Applied Sci., 3: 214-221. DOI: 10.3844/ajeassp.2010.214.221

Delgosha, F., 2009. A multivibrate key establishment scheme for wireless sensor networks. IEEE Trans. Wireless Commun., 18: 232-238. DOI: 10.1109/TWC.2009.071338

Djenouri, D. and L. Khelladi, 2005. A survey of security issues in mobile adhoc and sensor networks. IEEE Commun. Surv. Tutorials, 7: 2-28. DOI: 10.1109/COMST.2005.1593277

Fuchs, G., S. Truchat and F. Dressler, 2006. Distributed Software Management in Sensor Networks using Profiling Techniques. Proceedings of the 1st IEEE/ACM International Conference on Communication System Software and Middleware (IEEE COMSWARE 2006): 1st International Workshop on Software for Sensor Networks (SensorWare 2006), New Dehli, India, pp: 1-6. DOI: 10.1109/COMSWA.2006.1665225

Gaubatz, G., J.P. Kaps and B. Sunar, 2004. Public key cryptography in sensor networks revisited. Proceedings of the 1st European Workshop on Security in Ad-Hoc and Sensor Networks (ESAS 2004), pp: 2-18. http://citeseer.ist.psu.edu/viewdoc/summary?doi=10.1.1.101.7772

Hanapi, Z.M., M. Ismail and K. Jumari, 2009. Priority and random selection for dynamic window secured implicit geographic routing in wireless sensor network. Am. J. Eng. Applied Sci., 2: 494-500. DOI: 10.3844/ajeassp.2009.494.500

Ismail, N.M.H. and M. Othman, 2009. Low power phase locked loop frequency synthesizer for 2.4 ghz band zigbee. Am. J. Eng. Applied Sci., 2: 337-343. DOI: 10.3844/ajeassp.2009.337.343

Maalla, A., C. Wei and H.J. Taha, 2009. Optimal power multicast problem in wireless mesh networks by using a hybrid particle swarm optimization. Am. J. Applied Sci., 6: 1758-1762. DOI: 10.3844/ajassp.2009.1758.1762

Mbaitiga, Z., 2009. Intelligent OkiKoSenPBX1 security patrol robot via network and map-based route planning. J. Comput. Sci., 5: 79-85. DOI: 10.3844/jcssp.2009.79.85

Nardal, S. and A. Sahin, 2011. Ethical issues in e-commerce on the basis of online retailing. J. Soc. Sci., 7: 190-198. DOI: 10.3844/jssp.2011.190.198

Perrig, A., J. Stankovic and D. Wagner, 2004. Security in wireless sensor networks. Commun. ACM, 47: 53-57. http://www.cs.virginia.edu/papers/p53-perrig.pdf

Perrig, A., R. Szewczyk, V. Wen, D. Culler and J.D. Tygar, 2002. SPINS: Security protocols for sensor networks. Wireless Networks, 8: 521-534. DOI: 10.1023/A:1016598314198

Sundararajan and A. Shanmugam, 2010. A novel intrusion detection system for wireless body area network in health care monitoring. J. Comput. Sci., 6: 1355-1361. DOI: 10.3844/jcssp.2010.1355.1366

Vigilant, D., 2008. RSA with CRT: A new cost-effective solution to thwart fault attacks. Cryptographic Hardware Embedded Syst., 5154: 130-145. DOI: 10.1007/978-3-540-85053-3_9

Xiao, Y., V. Rayi, B. Sun, X. Du and F. Hue, 2007. A survey of key management schemes in wireless sensor networks. Comput. Commun., 30: 2314-2341. DOI: 10.1016/j.comcom.2007.04.009

Yang, H., H. Luo, F. Ye, S. Lu and L. Zhang, 2004. Security in mobile ad hoc networks: Challenges and solutions. IEEE Wireless Commun., 11: 38-47. DOI: 10.1109/MWC.2004.1269716