Security in Mobile Wireless Network with Less Storage Overhead

DR. JAYKUMAR SHANTILAL PATEL

Chaudhari Technical Institute, Sector-7, Gandhinagar, Gujarat, India

Email: jay_sp_mca@yahoo.co.in
Telephone: +91-9714064664

Abstract - Most of the recent trends in the robust security implementation attract the researcher towards the group communication using the session key. How to distribute a group session key securely in the unreliable wireless network is the most challenging task for researchers. Due to the unreliable broadcast nature of the mobile wireless network packet loss scenario occurs frequently. Furthermore, wireless mobile nodes are battery operated hence we have to be careful of battery life time. To acquire robust security symmetric and asymmetric key algorithms are there. Asymmetric algorithms are more secure comparing with the symmetric algorithms, but asymmetric algorithms are more complex and it requires large storage. The proposed research work is based on group theory, namely bilinear pairing on the Elliptic Curve point. The proposed work uses the concepts of asymmetric key for securely exchange key value with less storage overhead.

Keywords: Session key, Asymmetric key, Elliptic Curve, Storage overhead.

(Received June 1st, 2020/ Accepted June 11st, 2020)

1. Introduction

The mobile wireless environment consists of a large number of battery operated mobile wireless devices. These battery operated devices are more constraint base. The robust security implementation in such constraint based network is too much difficult compare to traditional network. Many differences have been observed between wireless sensor networks (WSN) and more traditional data communication networks; consequently, the algorithms, protocols and techniques used in traditional networks are not adequate for WSNs [1]. The challenges in this type of mobile wireless network are to reduce the storage, overhead so the battery consumption is as much possible as reduced because it is not feasible to frequently replace the batteries of large scale mobile devices. Security is an important feature of wireless network because mobile devices may relate to insightful data and operate in the hostile environment [2-6].

The proposed research considers the core concept of the security that is key management. The use of elliptic curve cryptography is to acquire robust security. The values of the public and private key pairs are nothing but the points on elliptic curves. The proposed research also uses the bilinear pairing operation, Hash calculation, MAC in terms of pseudo random function PRF and symmetric encryption for location secrecy and the nonce for key confirmation.

2. Literature Survey

Wireless Sensor Networks communicate by sending and receiving packets among one another [7]. It is important to provide security in wireless sensor networks so that only the correct user gets the message [7]. Cryptography is an important concept which provides security in Wireless Sensor Networks [7]. The development of wireless sensor networks was originally motivated by military applications for battlefield surveillance [8]. Thereafter, wireless sensor networks are used in many civilian application areas, including environment and habitat monitoring, health care applications, home automation, and traffic control [8]. A wireless network is energy efficiency, since a majority of wireless devices operate on batteries that need to be regularly recharged from a power source [9]. Wireless network comprises limitations in resources such as processing power, storage capacity, and communication range and power availability [1]. Nodes in sensor networks have restricted storage, computational and energy resources [10]. Additionally, these sensor nodes have limited processing power, storage and energy [10]. Low energy consumption, limited storage and memory usage are the three main constraints of wireless network [11]. Transmission reliability with energy efficiency makes the key for a good design in wireless sensor networks [9]. As in any traditional wireless sensor network, power consumption is a fundamental concern [9]. The convenience of use and freedom to move anywhere at anytime making the cellular wireless networks popular among the users. Mobility of the users also poses a challenge to the network engineers, for achieving the desired quality of service (QoS) [12]. For mobile nodes to connect each other in physically insecure environment, security is an essential aspect [13]. The security issue has been overlooked in the design of most of the default routing protocols [13]. Public key cryptography, provide practical solutions for information security in various situations [14]. There are two branches of modern cryptographic techniques: public-key or asymmetric cryptography and secret-key or symmetric cryptography [14]. Public-key cryptography is the technological revolution which solves the key distribution problem. It is based on a pair of asymmetric keys [14]. Asymmetric cryptography algorithms comprise Deffie-Hellman key exchange for secure communication by Deffi and Hellman [6] and Elliptic Curve Cryptography by Koblitz [15] and Millier [16]. Asymmetric cryptography algorithms normally involved the discrete exponential in cyclic group which will require large numbers of loops and lots of functions to execute the algorithm. Therefore Karlof et al. [17], Perrig, et al. [18]And Perrig, et al. [19] prohibits asymmetric cryptography algorithm on power constraint sensor nodes.. However, Watro et al. [20] provide the concept of shared key with a trusted base station in order to make the asymmetric key operation feasible under the constraint based sensor network. Malan, Welsh and Smith [21] claim that elliptic-curve cryptography (ECC) is more practical than Diffe-hellman, since it provides healthier attack resistance with a smaller prime modulus. This same result is supported by Piotrowski et al. [22] with finding that the energy require to perform RSA-1024 key generation is 360mj, while it requires only 27mj for ECC-160 to acquire an equivalence security level. There are schemes based on the framework of probabilistic key distribution [23-29] and recent study on applying public-key cryptography to sensor networks [30, 31].

Existing Scheme: Existing scheme proposed by Tian’s Scheme [32] has the value of storage cost (2dj+2d+3j+8)logq +16(d2+d+1)+2logq.

Where:

j = Number of session.

d = Number of users in session j

q = Number of bits.

log q = Number of bits used in the number of maximum size q.

3. Proposed Scheme

Preliminary:

No. of bits is directly calculated.

Log q means no. of bits used in the number of maximum size q.

The public key is nothing but the points (x1, y1) on elliptic curves. The value of a point on the curve is measured as log q. Here we have two points x1 and y1. So, log q + log q = 2logq.

Same way the private key is nothing but the points (x2, y2) on elliptic curves. The value of a point on the curve is measured as log q. Here we have two points x2 and y2.

So, log q + log q = 2logq.

In Proposed scheme:

Own Public key [ECC Point] =2logq bits

Own Private key [ECC Point] =2logq bits

GM Public key [ECC Point] =2logq bits

Own ID =logq bits

Session key (Kj) =logq bits

No. of session (m) [1 integer] =16 bits

Broadcast (Bj) [Bj have z1, z2, z3, … Zj]

z1, z2, z3, … zj have U, Ui, Vj

U [ECC Point] =2logq bits

Ui [where i=1 to d] [ECC point] =d(2logq) bits

Vj =logq bits

= J(2dlogq [For Ui] + 2logq [For U] + logq [For Vj])

= J(2dlogq + 2logq + logq)

=j(2dlogq + 3logq)

= j(2d + 3) logq

Total storage cost:

= j(2d+3) logq [For(7)] + 2logq [For (1)] + 2logq [For (2)] + 2logq [For (3)] + logq [For (4)] + logq [For (5)] + 16 [For (6)]

= j(2d + 3)logq + 2logq + 2logq + 2logq + logq + logq + 16

= j(2d + 3)logq + 8logq + 16

= (2dj + 3j)logq + 8logq +16

= (2dj + 3j + 8)logq + 16

4. Security Analysis

The security analysis of the proposed work is relay on five special properties: Forward

Secrecy, Backward Secrecy, Location Secrecy, Mutual Authentication, and Key Confirmation.

4.1. Forward Secrecy

Forward secrecy makes sure that a session key communicated by the source end to destination will not be compromised even though one of the session key in subsequent communication is compromised in the future [33].

4.2 Backward Secrecy

Backward secrecy makes sure that even if one session is compromised, it does not disclose the past session keys [33].

4.3. Mutual Authentication

To ensure the authentication source and destination nodes has to mutually authenticate each other. Pseudo Random Function PRF () is used to achieve mutual authentication.

4.4. Location Secrecy

Location secrecy achieved through implementation of confidentiality. Hence, during mutual authentication process unauthorized node may not able to be a part of real communication.

4.5 Key Confirmation

Key confirmation ensures that the distributed session key is delivered to intended recipient successfully. This phase validates the source for the successful delivery of session keys. Random value nonce is to set up the key confirmation phase.

5. Comparative Security Analysis

Following table 1 illustrate the comparison of various security features. The comparison is between proposed scheme and security schemes proposed by Tian et al [32], Varadharajan et al. [34], and Lee et al. [35].

	Lee et al. [35]	Varadharajan et al.[34]	Tian et al. [32]	Proposed Scheme
Forward Secrecy	No	No	Yes	**Yes**
Back-ward Secrecy	No	No	Yes	**Yes**
Mutual Authentication	No	No	No	**Yes**
Location Secrecy	No	No	No	**Yes**
Key Confirmation	No	No	No	**Yes**

Table 1 Comparison of Security Features

6. Performance Analysis

Evaluating the above comparative security analysis (Table 1) it is stated that Tian et al. [32] is far better than Lee et al. [35] and Varadharajan et al. [34]. Hence the proposed scheme is considered the Tian et al. [32] scheme for the various securities comparative.

Storage cost is a core to measure the performance of the proposed scheme. Each node stores its own public-private key pair and the group session keys for maximum m sessions. It also needs to temporarily store the broadcast message, which contains j ($1 \leq j \leq m$) entities. The proposed scheme saves storing cost of |Gj| X |Gj| matrix as well as it saves the storage cost to save public keys of all the nodes in group unlike Tian et al. [32].

Comparative Performance Analysis

Tian et al. [32]:

(2dj+2d+3j+8)logq+16(d2+d+1) + 2logq

Proposed Scheme:

(2dj+3j+8)logq+16

Where:

J = Session number ($1 \leq j \leq m$)

D = Number of users in session j

K = Number of neighbors to which a node responds for mutual healing in a session.

7. Result and Analysis

The proposed scheme calculates the storage cost through considering three core parameters such as the number of nodes, number of sessions and the prime number. These parameters are used to implement the Group theory. For the order of p (where p is large prime number) the group G1 and G2 are defined as additive and multiplicative group that saves far better storage compare with Tian et al. [32].

Number of Nodes (d): Numbers of nodes are proportional to storage values in proposed scheme as well as in the Tian et. al. [32] means storage values are increased when the number of nodes increased.

No. of Nodes	Storage Values (Bits)	
	Tian et al. [32]	Proposed Scheme

50	47939	5405
60	67059	6425
70	89379	7445
80	114899	8465
90	143619	9485
100	175539	10505

Table 2 Storage Values for Number of Nodes

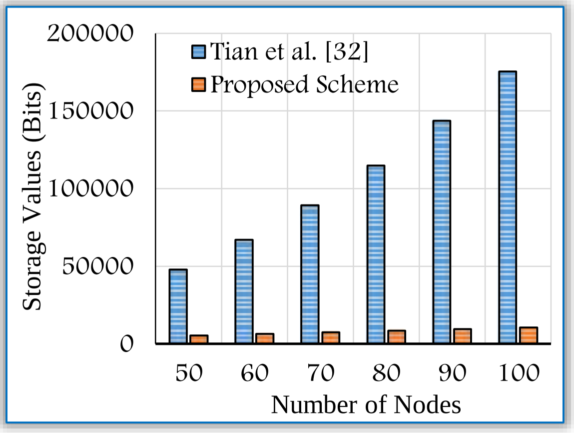

Figure 1 – Storage Values vs. No. of Nodes

No of Session (j): Numbers of sessions are proportional to storage values in proposed scheme as well as in the Tian et. al. [32] means storage values are increased when the number of sessions increased.

No. of Session	Storage Values (Bits)	
	Tian et al. [32]	Proposed Scheme
3	47939	5405
5	51441	8907
8	56694	14160
10	60196	17662
12	63698	21164
17	68951	26417

Table 3 Storage Values for Number of Sessions

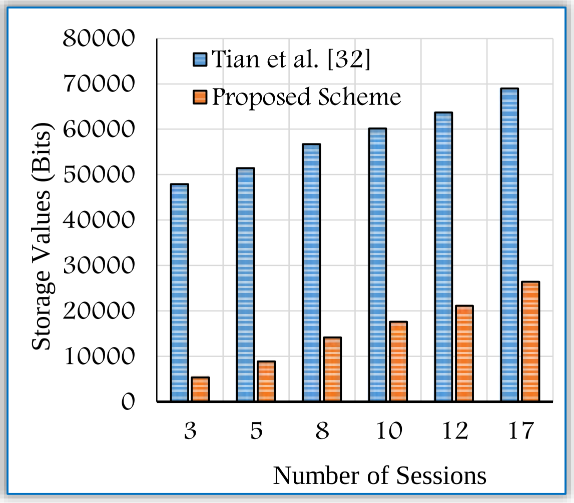

Figure 2 - Storage Values vs. No. of Sessions

Prime Number (q): Prime numbers are proportional to storage values in proposed scheme as well as in the Tian et. al. [32] means storage values are increased when prime numbers increased.

Prime Number	Storage Values (Bits)	
	Tian et al. [32]	Proposed Scheme
17	47939	5405
23	50453	7307
31	53805	9843
41	57995	13013
47	60509	14915
59	65537	18719

Table 4 Storage Values for Prime Numbers

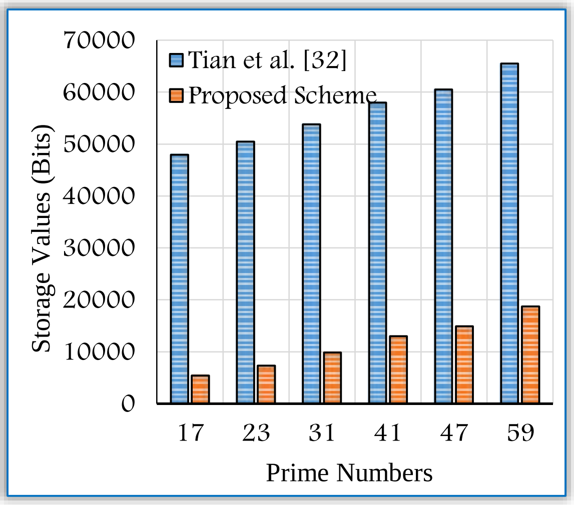

Figure 3 - Storage Values vs. Prime Numbers

8. Conclusion

The Proposed work provides robust security with less storage cost that saves the battery life. The research paper also shows the security analysis through Forward Secrecy, Backward Secrecy, Mutual Authentication, Location Secrecy and Key Confirmation. The result analysis done through three different approaches: various numbers of nodes, various numbers of sessions, various numbers of prime number. The result shows how miniaturize storage cost when value changes for nodes, sessions and prime number.

9. Future Enhancement

In future the proposed work should be extended to reduce the computational overhead and communication overhead. The extension done through enhancing security level in constraint based mobile wireless devices adhering the lifetime of the battery.

10. References

[1] Luis Enrique Palafox-Maestre and Jose Antonio Garcia-Macias, “A bio-inspired approach for data dissemination in wireless sensor networks”, INFOCOMP Journal of Computer Science, Vol. 5 No. 3, Page No: 19-27, September, 2006.

[2] I. Kasimoglui and F. Akyildiz, “Wireless sensor and actor: research challenges”, Elsevier Journal, 2(38), Page No: 351-367, 2004.

[3] S. Vaidynathan, S. Suri, and Sinha, ”Data aggregation techniques in sensor networks”, Technical Report, OSU-CISRC-11/04-TR60, 2004.

[4] D. Agrawal, N. Shrivastava, C. Buragohain, and S. Suri, “Medians and beyond: new aggregation techniques for sensor networks”, Proceedings of the 2nd international conference on Embedded networked sensor systems, Page No: 239-249, ACM Press, 2004.

[5] P. Nair, H. Cam, S. Ozdemir, and D. Muthuavinashiappan, “Espda: Energy efficient and secure pattern based data aggregation for wireless sensor networks”, Computer Communications IEEE Sensors, Page No: 446-455, 2006.

[6] W. Diffe and M. Hellman, “New directions in cryptography”, IEEE Transactions on Information Theory, Vol. 22, Page No: 644-654, November, 1976.

[7] Bannishikha Banerjee and Jalpa T Patel, “A Symmetric Key Block Cipher to Provide Confidentiality in Wireless Sensor Networks”, INFOCOMP Journal of Computer Science, Vol. 15 No. 1, Page No: 12-18, June 2016.

[8] Elbhuru Brahim, Saadane Rachid, Alba-Pagès Zamora and Driss Aboutajdine, “Stochastic and Balanced Distributed Energy-Efficient Clustering (SBDEEC) for Heterogeneous Wireless Sensor Networks”, INFOCOMP Journal of Computer Science, Vol. 8 No. 3, Page No: 11-20, September, 2009.

[9] Mohamed K. Watfa and Farah Abou Shahla, “Energy-Efficient Scheduling in WMSNs”, INFOCOMP Journal of Computer Science, Vol. 8 No. 1, Page No: 45-54, March, 2009.

[10] R. Vidhyapriya and P. T. VanathiLiguo Yu, “Energy Aware Routing for Wireless Sensor Networks”, INFOCOMP Journal of Computer Science, Vol. 6 No. 3, Page No: 7-14, September, 2007.

[11] Mohamed Watfa, Wiliiam Daher and Hisham al Azar, “An Energy Aware Sensor Network Query Processing System”, INFOCOMP Journal of Computer Science, Vol. 8 No. 1, Page No: 37-44, March, 2009.

[12] Rajkumar Samanta, Partha Bhattacharjee and Gautam Sanyal, “QoS Evaluation of Cellular Wireless Networks with Non-Classical Traffic and Queuing Handoff Requests”, INFOCOMP Journal of Computer Science, Vol. 9 No. 4, Page No: 11-20, December, 2010.

[13] Rutvij H. Jhaveri, Sankita J. Patel and Devesh C. Jinwala, “Improving Route Discovery for AODV to Prevent Blackhole and Grayhole Attacks in MANETs”, INFOCOMP Journal of Computer Science, Vol. 11 No. 1, Page No: 1-12, March, 2012.

[14] N. L. Gupta, D. R. Mehrotra and Ashutosh Saxena, “Quantum Cryptographic Protocols for Secure Comunication”, INFOCOMP Journal of Computer Science, Vol. 8 No. 1, Page No: 65-74, March, 2009.

[15] N. Koblitz, “Elliptic curve cryptosystems Mathematics of Computation”, Vol. 48, No. 177, Page No: 203-209, 1987.

[16] V. Miller, “Use of elliptic curves in cryptography”, CRYPTO 85 Proceedings: Advances in Cryptology, Page No: 417-426, 1986.

[17] C. Karlof, N. Sastry, and D.Wagner, “TinySec: a link layer security architecture for wireless sensor networks”, SenSys 2004: Proceedings of the 2nd International Conference on Embedded Networked Sensor Systems, (New York, NY, USA), Page No: 162-175, ACM, November, 2004.

[18] A. Perrig, J. Stankovic, and D. Wagner, “Security in wireless sensor networks Communications”, ACM, Vol. 47, No. 6, Page No: 53-57, 2004.

[19] A. Perrig, R. Szewczyk, J. Tygar, V. Wen, and D. Culler, “SPINS: Security Protocols for Sensor Networks Wireless Networks”, Vol. 8, No. 5, Page No: 521-534, 2002.

[20] R. Watro, D. Kong, S. Cuti, C. Gardiner, C. Lynn, and P. Kruus, “TinyPK: securing sensor networks with public key technology”, SASN '04: Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks, (New York, NY, USA), Page No: 59-64, ACM, 2004.

[21] D. Malan, M. Welsh, and M. Smith, “A public-key infrastructure for key distribution in TinyOS based on elliptic curve cryptography”, IEEE SECON 2004: First Annual IEEE Communications Society Conference on Sensor and Ad Hoc Communications and Networks, pp. 71-80, October, 2004.

[22] K. Piotrowski, P. Langendoerfer, and S. Peter, “How public key cryptography influences wireless sensor node lifetime”, SASN '06: Proceedings of the fourth ACM workshop on Security of ad hoc and sensor networks, (New York, NY, USA), Page No: 169-176, ACM, 2006.

[23] L. Eschenauer and V. Gligor, “A Key-Management Scheme for Distributed Sensor Networks”, in Proceedings of ACM CCS’02, 2002.

[24] H. Chan, A. Perrig, and D. Song, “Random Key Pre-distribution Schemes for Sensor Networks”, in Proceedings of IEEE Security and Privacy Symposim’03, 2003.

[25] W. Du, J. Deng, Y. Han, and P. Varshney, “A Pairwise Key Pre distribution Scheme for Wireless Sensor Networks”, in Proceedings of the 10th ACM Conference on Computer and Communications Security (CCS’03), Page No: 42–51, 2003.

[26] R. Pietro, L. Mancini, and A. Mei, “Random Key Assignment for Secure Wireless Sensor Networks”, in Proceedings of ACM Workshop SASN, 2003.

[27] S. Zhu, S. Xu, S. Setia, and S. Jajodia, “Establishing Pair-wise Keys For Secure Communication in Ad Hoc Networks: A Probabilistic Approach”, in Proceedings of 11th IEEE International Conference on Network Protocols (ICNP’03), 2003.

[28] D. Liu and P. Ning, “Location-Based Pair wise Key Establishments for Static Sensor Networks”, Proceedings of 2003 ACM Workshop on Security in Ad Hoc and Sensor Networks (SASN ’03), 2003.

[29] H. Chan and A. Perrig, “PIKE: Peer Intermediaries for Key Establishment in Sensor Networks”, in the 24th Conference of the IEEE Communications Society (Infocom 2005), 2005.

[30] A. Wacker, M. Knoll, T. Heiber, and K. Rothermel, “A New Approach for Establishing Pairwise Keys for Securing Wireless Sensor Networks”, in Proceedings of ACM SenSys, 2005.

[31] K. Simonova, A. Ling, and X. Wang, “Location-aware key pre-distribution scheme for wide area wireless sensor networks”, in Proceedings of ACM SASN Workshop, 2006.

[32] B. Tian, S. Han, J. Hu, and T. Dillon, “A mutual-healing key distribution scheme in wireless sensor networks”, Journal of Network and Computer Applications, Vol. 34, Issue 1, Page No: 80-88, 2018.

[33] Peter Hillmann, Marcus Knüpfer, Tobias Guggemos and Klement Streit, “CAKE: An Efficient Group Key Management for Dynamic

Groups”, INFOCOMP Journal of Computer Science, Vol. 18 No. 2, Page No: pp-pp, December 2019.

[34] V. Varadharajan, R. Shankaran, and M. Hitchens, “Security for cluster based ad hoc networks”, Computer Communications, Vol. 27, No. 5, Page No: 488-501, 2004.

[35] J. Lee and C. Chang, “Secure communications for cluster-based ad-hoc networks using node identities”, Journal of Network and Computer Applications, Vol. 30, No. 4, Page No: 1377-1396, 2007.