International Journal of Contemporary Research in Computer Science and Technology (IJCRCST) e-ISSN: 2395-5325
Volume1, Issue 7 (October '2015)

A SURVEY ON IDENTIFICATION SERVICE TECHNIQUES ON DES AND MARKLE HASH TREE IN WIRELESS SENSOR NETWORK

M.Kavitha,
M.Phil scholar,
Sengunthar Arts & Science College,
Tiruchengode, Tamilnadu,India.

P.Balamurugan,
Assistant Professor,
Sengunthar Arts & Science College,
Tiruchengode, Tamilnadu,India.

Abstract: Wireless sensor networks have enabled data gathering from a huge geographical region, and present unprecedented opportunities for a wide range of tracking and monitoring applications from both civilian and military domains.WSN can be viewed as a closed user group and therefore the application of symmetric cryptography seems sufficient. However, since sensor nodes are often deployed in an unattended or even hostile environment, an adversary may compromise a sensor node to access stored keys and compromise the security of the communication in the whole group. If a query result that a storage node sends to the sink includes forged data or excludes legitimate data, the query result is guaranteed to be detected by the sink as invalid. In this paper we get survey of more integrity techniques also we discussed about Symmetric Key Encryption Techniques.

Keywords: Wireless sensor Networking, privacy, integrity, Encryption, symmetric key

I.INTRODUCTION

A wireless network, which uses high-frequency radio waves rather than wires to communicate between nodes, is another option for home or business networking. Individuals and organizations can use this option to expand their existing wired network or to go completely wireless. Wireless allows for devices to be shared without networking cable which increases mobility but decreases range [1] [2]. Ad-hoc or peer-to-peer wireless network consists of a number of computers each equipped with a wireless networking interface card. Each computer can communicate directly with all of the other wireless enabled computers [3]. They can share files and printers this way, but may not be able to access wired LAN resources, unless one of the computers acts as a bridge to the wired LAN using special software. A wireless sensor networks (WSNs) consists of spatially distributed autonomous sensors to monitor physical or environmental conditions, such as temperature, sound, pressure, etc. and to cooperatively pass their data through the network to a main location.

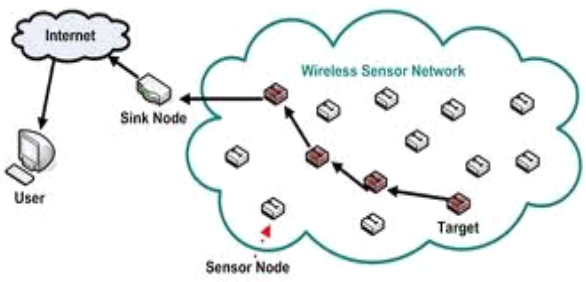

Figure 1 Wireless Sensor Networks

The more modern networks are bi-directional, also enabling control of sensor activity. Nodes are equipped with radio transceiver, processing unit, battery and sensor(s). Wireless sensor networks as show in figure 1. Nodes are constrained in processing power and energy, whereas the sink node is not severely energy resources. The sink node act as gateways between the WSN and other networks such as Internet etc.

WSNs are becoming one of the building blocks of pervasive computing. It provides simple and cheap mechanism for monitoring in the specified area. But WSN technology is an inappropriate use can significantly violate privacy of humans. WSNs are frequently deployed to collect sensitive information. WSN can be used to monitor the movements of traffic in a city. Such a network can be used to determine location of people or vehicles. The sensor nodes such networks are deployed over a geographic area by aerial scattering or other means. Each sensor node can only detect events within a very limited distance, called the sensing range.

II. SECURITY IN WIRELESS SENSOR NETWORKS

Network Security and Cryptography is a concept to protect network and data transmission over wireless network [16]. Data Security is a challenging issue of data communications today that touches many areas including secure communication channel, strong data encryption technique and trusted third party to maintain the database. The conventional methods of encryption can only maintain the data security. The information could be accessed by the unauthorized user

for malicious purpose.

Therefore, it is necessary to apply effective encryption/decryption methods to enhance data security.

A). Security Requirements

A sensor network is a special type of network. It shares some commonalities with a typical computer network.

Data Confidentiality: Data confidentiality is the most important issue in network security. Every network with any security focus will typically address this problem first. In sensor networks, the confidentiality relates to the following:

- A sensor network should not leak sensor readings to its neighbors. Especially in a military application, the data stored in the sensor node may be highly sensitive.
- In many applications nodes communicate highly sensitive data, e.g., key distribution; therefore it is extremely important to build a secure channel in a wireless sensor network.
- Public sensor information, such as sensor identities and public keys, should also be encrypted to some extent to protect against traffic analysis attacks.

Data Integrity: With the implementation of confidentiality, an adversary may be unable to steal information. However, this doesn't mean the data is safe. The adversary can change the data, so as to send the sensor network into disarray. For example, a malicious node may add some fragments or manipulate the data within a packet. This new packet can then be sent to the original receiver. Data loss or damage can even occur without the presence of a malicious node due to the harsh communication environment. Thus, data integrity ensures that any received data has not been altered in transit.

Data Freshness: Even if confidentiality and data integrity are assured, it also needs to ensure the freshness of each message. Informally, data freshness suggests that the data is recent, and it ensures that no old messages have been replayed.

Availability: The availability of a sensor and sensor network for the following reasons:

- Additional computation consumes additional energy. If no more energy exists, the data will no longer be available.
- Additional communication also consumes more energy. What's more, as communication increases so too does the chance of incurring a communication conflict.
- A single point failure will be introduced if using the central point scheme. This greatly threatens the availability of the network.

Time Synchronization: Most sensor network applications rely on some form of time synchronization. In order to conserve power, an individual sensor's radio may be turned off for periods of time.

Authentication: An adversary is not just limited to modifying the data packet. It can change the whole packet stream by injecting additional packets. So the receiver needs to ensure that the data used in any decision-making process originates from the correct source. On the other hand, when constructing the sensor network, authentication is necessary for many administrative tasks (e.g. network reprogramming or controlling sensor node duty cycle). From the above, it can see that message authentication is important for many applications in sensor networks. Informally, data authentication allows a receiver to verify that the data really is sent by the claimed sender. In the case of two-party communication, data authentication can be achieved through a purely symmetric mechanism: the sender and the receiver share a secret key to compute the message authentication code (MAC) of all communicated data.

B). Security Mechanisms for Wireless Sensor Networks

Security mechanisms are (i) cryptographic mechanisms, (ii) Both public key cryptography and symmetric key cryptographic techniques, (iii) A number of key management protocols, (iv) Secure data aggregation mechanisms for WSN security.

Cryptography in WSNs: Selecting the most appropriate cryptographic method is vital in WSNs as all security services are ensured by cryptography. Cryptographic methods used in WSNs should meet the constraints of sensor nodes and be evaluated by code size, data size, processing time, and power consumption.

Public Key Cryptography in WSNs: Many researchers believe that the code size, data size, processing time, and power consumption make it undesirable for public key algorithm techniques, such as the Diffie-Hellman key agreement protocol or RSA signatures to be employed in WSNs. Public key algorithms such as RSA are computationally intensive and usually execute thousands or

even millions of multiplication instructions to perform a single-security operation. Further, a microprocessor's public key algorithm efficiency is primarily determined by the number of clock cycles required to perform a multiplication instruction.

Symmetric Key Cryptography in WSNs: Most of the public key cryptographic mechanisms are computationally intensive, most of the research studies for WSNs focus on use of symmetric key cryptographic techniques. Symmetric key cryptographic mechanisms use a single shared key between the two communicating host which is used both for encryption and decryption. However, one major challenge for deployment of symmetric key cryptography is how to securely distribute the shared key between the two communicating hosts. This is a non-trivial problem since pre-distributing the key may not always be feasible. Five popular encryption schemes are: RC4, RC5, IDEA, SHA-1, and MD5.

Key Management Protocols: The area that has received maximum attention of the researchers in WSN security is key management. Key management is a core mechanism to ensure security in network services and applications in WSNs. The goal of key management is to establish the keys among the nodes in a secure and reliable manner. In addition, the key management scheme must support node addition and revocation in the network. Since the nodes in a WSN have computational and power constraints, the key management protocols for these networks must be extremely light-weight.

Key Management on Probability of Key Sharing: The key management protocols for WSNs may be classified on the probability of key sharing between a pair of sensor nodes. Depending of this probability the key management schemes may be either deterministic or probabilistic.

Secure Data Aggregation: An efficient data aggregation mechanism can greatly help in optimizing the energy consumption**.** In a WSN, there are certain nodes called aggregators which are responsible to carry out data aggregation operations**.** If an aggregator node is compromised, it is easy for an adversary to inject false data into the network. Another possible attack is to compromise a sensor node and inject forged data through it. Without authentication, the attackers may fool the aggregators into reporting false data to the base station. Secure data aggregation requires authentication, confidentiality, and integrity [4].

III.LITERATURE REVIEW

Wenliang Du., et al., described a Key Management Scheme for Wireless Sensor Networks using Deployment Knowledge [5] in 2004. In existing, Pre-distribution of secret keys for all pairs of nodes is not viable due to the large amount of memory used when the network size is large. It is not suitable for wireless sensor networks. Due to this reason, this paper proposed a Random key pre-distribution scheme is that no deployment knowledge is available. Random key pre-distribution scheme that exploits deployment knowledge and avoids unnecessary key assignments. This proposed scheme reduction in memory usage not only relieves the memory requirement on the memory-constrained sensor node, it substantially improves network's resilience against node capture. In further improvement how much the deployment knowledge can improve the q-composite random key pre-distribution scheme and the pairwise key pre-distribution scheme.

Donggang Liu et al., introduced Establishing Pairwise Keys in Distributed Sensor Networks [6] in 2005. Pairwise key establishment is infeasible to use traditional management techniques such as public key cryptography and key distribution center (KDC). Due to this reason, the proposed work implemented two efficient instantiations of the general framework: a random subset assignment key predistribution scheme and a grid-based key predistribution scheme. These two schemes provided a high probability (or guarantee) to establish pairwise keys, tolerance of node captures, and low communication overhead. The grid-based scheme can be suggested for easily extended to an n-dimensional or hypercube based scheme.

Dawn Xiaodong Song David Wagner [7] performed Practical Techniques for Searches on Encrypted Data in 2000. It is desirable to store data on data storage servers such as mail servers and file servers in encrypted form to reduce security and privacy risks. But this usually implies that one has to sacrifice functionality for security. Due to this reason, cryptographic schemes are implemented for the problem of searching on encrypted data and provide proofs of security for the resulting crypto systems. The techniques provide provable secrecy for encryption, in the sense that the untrusted server cannot learn anything about the plaintext it given only the ciphertext. Asymmetric key cryptographic techniques could be suggested for providing secrecy and encryption.

Premkumar, Devanbu, et al., [8], developed Authentic Data Publication over the Internet in 2003. Integrity critical databases, such as financial information used in high-value decisions, are frequently published over the Internet. Publishers of such data must satisfy the integrity, authenticity,

and non-repudiation requirements of clients. Providing this protection over public data networks is an expensive proposition. This is the difficulty of building and running secure systems. In practice, large systems cannot be verified to be secure and are frequently penetrated. The negative consequences of a system intrusion at the publisher can be severe. The problem is further complicated by data and server replication to satisfy availability and scalability requirement. Due to this problem merkle hash trees could be suggested that publishers can used to provide authenticity and non-repudiation of the answer to database queries posed by a client.

Bijit Hore, et al., [9], introduced A Privacy-Preserving Index for Range Queries in 2004. Database outsourcing is an emerging data management paradigm, which has the potential to transform the IT operations of corporations. To address privacy threats in database outsourcing scenarios where trust in the service provider is limited. Due to this reason, this paper analyzes the data partitioning (bucketization) technique and it also algorithmically developed to build privacy-preserving indices on sensitive attributes of a relational table.

Ronald Watro, et al., described TinyPK: Securing Sensor Networks with Public Key Technology [10] in 2004**.** The communication security problems for sensor networks are exacerbated by the limited power and energy of the sensor devices. The critical problem is making effective use of that secure symmetric encryption capability. Public key (PK) technology is a widely used tool to support symmetric key management in the realm of Internet hosts and high-bandwidth interconnections. In this paper proposed the design and implementation of public-key-(PK)-based protocols that allow authentication and key agreement between a sensor network and a third party as well as between two sensor networks.

Bo Sheng and Qun Li introduced Verifiable Privacy-Preserving Range Query in Two-tiered Sensor Networks [11] in 2008. It considered a sensor network that is not fully trusted and asks the question how we preserve privacy for the collected data and how to verify the data reply from the network. Due to this problem, the context of a network augmented with storage nodes and target at range query. Bucketing scheme can be suggested to mix the data for a range, use message encryption for data integrity, and employ encoding numbers to prevent the storage nodes from dropping data.

Roberto Di et.al proposed Location Privacy and Resilience in Wireless Sensor Networks Querying [12] in 2010. It provided a probabilistic algorithm and scalable protocol to compute the MAX that enjoys the following features: (i) it guarantees the location privacy of the sensors replying to the query; (ii) it is resilient to an active adversary willing to alter the readings sent by the sensors; and, (iii) it allows to trade-off the accuracy of the result with (a small) overhead increase.

Xueying Zhang et al., developed Energy Efficiency of Symmetric Key Cryptographic Algorithms in Wireless Sensor Networks [13] in 2010. In this paper proposed, examined the energy efficiency of symmetric key cryptographic algorithms applied in wireless sensor networks (WSNs). It derives the computational energy cost of the ciphers under consideration by comparing the number of CPU cycles required to perform encryption. After evaluating a number of symmetric key ciphers, it compared the energy performance of stream ciphers and block ciphers applied to a noisy channel in a WSN.

Subhankar Chattopadhyay et al., introduced A Scheme for Key Revocation in Wireless Sensor Networks [14] in 2010. In existing, Centralized key revocation has a single point of failure. Due to this reason this paper proposed a key revocation scheme based on voting procedure is distributed key revocation algorithm. It represented all the keys of a compromised node can be successfully revoked from the entire network. In future, any other mechanism can be used for voting technique so further reduce the storage cost and time to revoke a compromised node. Also future improvements can be made in terms of reducing the computational and communication cost.

Anderson Santana de performed Privacy-Preserving Techniques and System for Streaming Databases [15] in 2012. In this proposed work considered high performance symmetric encryption techniques for greater-than and range queries based on Bloom filters; a system implementation of privacy-preserving event correlation based on MXQuery [maximum query] and a systematic performance evaluation of symmetric encryption techniques allowing equality tests, range queries, and blind addition. Proto-filter could be suggested for optimize the key distribution and event generation for different types of queries.

Qiang ZHOU developed A Novel Integrity-preserving Privacy Data Aggregation in Sensor Networks [16] in 2012. Data privacy and integrity preserving play important roles in wireless sensor networks (WSNs). Wireless sensor networks should have the function of privacy preserving and integrity checking in data aggregation. In this paper proposed a novel integrity-preserving privacy data aggregation in sensor networks, which is called IPPDA. First, the "slicing and

assembling" technique is implemented to provide privacy preserving; then aggregation nodes perform delayed aggregation, which trades off a slight increase in communication overhead in return for the ability to execute integrity checking; and then the child monitoring mechanism is adopted to detect the location of bogus data, remove the compromised node and eliminate communication overhead caused by bogus data. Secure data aggregation schemes can be suggested for general aggregation functions.

Fei Chen and Alex X. Liu [17], performed Privacy and Integrity Preserving Range Queries in Sensor Networks in 2012. In sensor networks, storage node function act as an intermediate between sensor and a sink for storing data and processing queries. It has been widely adopted because of the benefits of power and storage saving for sensors as well as the efficiency of query processing. The problem of this approach is the attackers hack the storage node. To prevent attackers from gaining information from both sensor collected data and sink issued queries. The encryption procedure is introduced to encode each data and queries specified by a storage node. This properly by using data encryption standard algorithm. Data encryption standard (DES) procedure is easy to possible to attack. RSA (Rivest Shamir Adleman) algorithm can be suggested for protecting data and queries.

IV. PRIVACY AND INTEGRITY TECHNIQUES BASED ON DES

Data Privacy is a challenging issue for data communications today that touches many areas including secure communication channel, strong data encryption technique and trusted third party to maintain the database. The conventional methods of encryption can only maintain the data security. Types of Encryption Method, Symmetric key Encryption and Asymmetric key Encryption.

A) Symmetric Key Encryption

Symmetric key cryptographic mechanisms used a single key between the two communicating host which is used both for encryption and decryption. One major challenge for deployment of symmetric key cryptography is securely distribute the single key between the two communicating hosts. This is a non-trivial problem since pre-distributing the key may not always be feasible.DES algorithm is a symmetric key Encryption Mechanism. The Data Encryption Standard (DES) also called as the Data Encryption Algorithm (DEA) by ANSI and DEA-1 by ISO. A cryptographic algorithm used for over three decades. DES , Double DES and Trible DES[18].

(i). Data Encryption Standard: DES is a block cipher as show in figure 4.1. Encrypts data in blocks of size 64 bits each. 64 bits of plain text goes as the input to DES, which produces 64 bit of cipher text the same algorithm and key are used for encryption and decryption, with minor differences. The key length is 56 bits.

- To encrypt plain text (P) with key (k1) then produces cipher text (C) C = Ek1 (P)
- To decrypt cipher text (C) with key (k1) then produces plain text (P) P = Dk1 (C)56-bit key

Data Encryption Standard Algorithm

Step 1:	In the first step, the initial 64-bit plain text block is handed over to Initial Permutation (IP) function.
Step 2:	The Initial permutation is performed on plain text.
Step 3:	The initial permutation produces two halves of permuted block: Left Plain text (LPT) and Right Plain (RPT).
Step 4:	Now, each of LPT and RPT goes through 16 rounds of the encryption process, each with its own key: a. From the 56-bit key, a different 48-bit Sub-key is generated using Key Transformation. b. Using the Expansion Permutation, the RPT is expended from 32 bits to 48 bits. c. Now, the 48-bit key is XORed with 48-bit RPT and the resulting output is given in the next step. d. Using the S-box substitution produce the 32-bit from 48-bit input. e. These 32 bits are permuted using P-Box Permutation.
Step 5:	f. The P-Box output 32 bits are XORed with the LPT 32 bits. g. The result of the XORed 32 bits is becomes the RPT and old RPT become the LPT. This process is called as swapping. h. Now the RPT again given to the next round and performed the 15 more rounds. After the completion of 16 rounds the Final Permutation is performed.

Variations of DES: The DES is susceptible to possible attacks. However, because DES is already proven to be a very competent algorithm, it would be nice to reuse DES by making it stronger by some means. Rather than writing a new cryptographic algorithm. Writing a new algorithm is not easy, more so because it has to be tested sufficiently so as to be proved as a strong algorithm. Consequently the two main variation of DES have emerged, which are Double DES and Triple DES.

(ii). Double DES: Double DES is quite simple to understand. Essentially, it does twice what DES normally does only once. Double DES uses two keys, says k1and k2. It first performs DES on the original plain text using k1 to get the encrypted text. It again performs DES on the encrypted text, but this time with the other key k2. The final output is the encryption of encrypted text.

$$C = Ek2 (Ek1 (P))$$
$$P = Dk2 (Dk1 (C))$$

(iii). Triple DES: In triple DES the plain text P is encrypted with a key k1, then encrypted with a second key k2, and finally encrypted with a key k3. Where k1, k2 and k3 are all different from each other [41].

$$C = Ek3 (Ek2 (Ek1 (P)))$$
$$P = Dk3 (Dk2 (Dk1 (C)))$$

The key length of 3DES is 168 bits three times as large as with DES (56 bits), making the key complexity by a factor of $2^{112}$is increased. The effective key length is 112 bits but only due to the possibility of the so-called meet-in -the-middle attack: If the attacker in possession of a pair of plain text and cipher, so attacker can attack the encryption of both sides. The plain text is all possible keys for encrypted (2^{56} possibilities). The resulting texts are also with all possible keys for each level 2 encrypted (2^{112} possibilities). Their results are compared with the results of decryption of the cipher text with all keys (2^{56} possibilities). So overall have only 2^{112} +2^{56} encryption and decryption are performed, instead of 2168 when using the brute force method[19].

V.CONCLUSION

We present a security and cryptography techniques of wireless sensor networks, and also discussed many researched in the field of security. Here we learn the problem of identification like privacy and integrity. Data privacy means that a storage node cannot know the actual values of sensor collected data. This ensures that an attacker cannot understand the data stored on a compromised storage node. Query privacy means that a storage node cannot know the actual value of sink issued queries. This ensures that an attacker cannot understand, or deduce useful information from, the queries that a compromised storage node receives.

VI.REFERENCES:

[1] Craig Zacker, "The Complete Reference Networking", Tata McGraw-Hill Edition, 2008.

[2] Andreas F.Molisch, "Wireless Communications", Second Edition, John Wiley and Sons Ltd., 2012.

[3] I.A.Dhotre, "Computer Networks", First Edition, Technical Publications, 2008.

[4] Kemal Akkaya and Mohamed Younis, "A Survey on Routing Protocols for Wireless Sensor Networks", Proceedings of the IEEE International Conference on Ad-Hoc Networks, November 2003.

[5] Wenliang Du, Jing Deng, Yunghsiang S. Han, "A Key Management Scheme for Wireless Sensor Networks Using Deployment Knowledge", Proceeding of the International Conference of the IEEE Computer and Communications Societies, Volume 1, March 2004.

[6] Donggang Liu, PengNing, Rongfang Li, "Establishing Pairwise Keys in Distributed Sensor Networks", Proceedings of the 10th ACM Conference on Computer and Communications Security, New York, 2005, pp 52-61.

[7] Dawn Xiaodong, Song David Wagner, Adrian Perri, "Practical Techniques for Searches on Encrypted Data", Proceedings of the IEEE Symposium on Security and Privacy, New York, May 2000.

[8] Premkumar, Devanbu, "Authentication Data Publication over the Internet", Journal of Computer Security, Volume 11, Issue 3, March 2003, pp 291-314.

[9] BijitHore, SharadMehrotra, Gene Tsudik, "A Privacy-Preserving Index for Range Queries", Proceedings of the International Conference on Very Large Databases, Volume 30, 2004, pp 720-731.

[10] Ronald Watro, Derrick Kong, Sue-fen Cuti, Charles Gardiner, "TinyPK: Securing Sensor Networkswith Public Key Technology", Proceedings of the second ACM Workshop on Security of Ad Hoc and Sensor Network, New York, 2004, pp 59-64.

[11] Bo Sheng, Qun Li, "Verifiable Privacy Range Query in Two-Tiered Sensor Networks", Proceedings of the 27th IEEE conference on Computer Communication, April 2008.

[12] Roberto Di Pietro, Alexandre Viejo, "Location Privacy and Resilience in Wireless Sensor Networks Querying", International Journal of Computer Security and Communications, Volume 34, Issue 3, 15 March 2011, pp 515-523.

[13] Xueying Zhang, HeysH.M,Cheng Li, "Energy Efficiency of Symmetric Key Cryptographic Algorithms in Wireless Sensor Networks", Proceedings of the 25th Biennial Symposium on Communications,

May 2010, pp 168-172.

[14] Subhankar Chattopadhyay, "A Scheme for Key Revocation in Wireless Sensor Networks", International Journal on Advanced Computer Engineering and Communication Technology, Volume 1, Issue 2, 2010.

[15] Anderson Santana de Oliveira, Hoon Wei Lim, Su-Yang Yu, "Privacy-Preserving Techniques and System for Streaming Databases", Proceeding of the International Conference on Social Computing, 5 September 2012, pp 728-733.

[16] Qiang Zhou, "A Novel Integrity- Preserving Data Aggregation in Sensor Networks", Journal of Computational Information Systems, Volume 8, Issue 20, Oct 2012, pp 8471-8478.

[17] Fei Chen and Alex X. Liu, "Privacy and Integrity Preserving Range Queries in Sensor Networks", Proceeding of the IEEE International Conference on Computer Communications, December 2012.

[18] Al-Sakib Khan Pathan, "Security in Wireless Sensor Networks: Issues and Challenges", Proceedings of the 8th IEEE International Conference, Volume 2, March 2006, pp 1043-1048.

[19] Gurpreet Singh, Supriya, "A Study of Encryption Algorithm (RSA, DES, 3DES and AES) for Information Security", International Journal of Computer Application, Volume 67, Issue19, April 2013.

