A Comprehensive Analysis of Security Issues and Cryptographic Paradigms in Wireless Ad hoc Sensor Networks

Abhishek Kumar
Abhisheikh.kmr@gmail.com

***Abstract*— The proliferation of Ad hoc sensor networks in various application scenarios has ostensibly called for effective security mechanisms. A lot of effort has been put and research has been carried out to tackle various threats that breach the security goals of the network. Since Wireless Sensor Network (WSN) does not rely on a concrete infrastructure and often deployed in hostile and irregular environments, its security requirement also differs vastly with that of traditional networks. It, thus, becomes imperative to design cryptographic algorithms that works efficiently keeping in mind the inherent limitations and constraints on resources, computational capability. In this paper, we present a survey on various security challenges of WSN and mechanisms to tackle the same. The aim is to present an extensive literature upon which research on security in WSN can be carried out.**

Keywords*— *WSN Security threats, Goals, Cryptographic algorithms

I. INTRODUCTION

Wireless ad hoc sensor networks consist of a very large number of small sensor nodes who are deployed in a certain area and work on multiple hop connect ad hoc basis. A sink node, which acts as a centralized base radio station receives data from all sensor nodes and forward them to gateway to deliver it to the external network. The main goal of designing these sensors, prima facie, is to make it cost efficient. And thus the sensor nodes have very limited processing ability, computational ability minimal power supply and limited storage. Since the conduit of communication is often unreliable and not monitored, the threats to security is behemoth. This fact coupled with mentioned factors pose a major challenge to the security aspects of the WSN. Even if we assume that the nodes operate in a cooperative manner and a trust is being maintained between them, the network and communication still is vulnerable to various threats and attacks.

The organization of this article is as follows: Inherent limitations to security, various security goals, attacks and threats, and various cryptographic algorithms and techniques to tract the security issues followed by a conclusion.

II. INHERENT LIMITATIONS TO SECURITY

The nature of ad hoc sensor networks and design of sensors make it difficult to employ existing security and cryptography algorithms to ensure security.so lets first figure out what those limitations are[1] and how they inhibit security. We will also understand how the security environment in WSN is different from that of traditional wired or ad hoc networks.

A. Limited Available Resources

The sensor nodes have very limited resources at their disposal such as little storage facility, less memory, limited power consumption. So with these limitations it's also an absolute necessity that the size of the cryptography algorithm should also be small and less computationally complex. We also need to consider the affect that the algorithm has on the battery consumption of node. A heavy weight cryptographic algorithm may drain the power of nodes soon and thus make them inefficient for other functions.

The communication in ad hoc sensor networks is often connectionless and thus unreliable. The probability of packet being damaged in transit and dropped due to congestion is fairly high. Also due to high bit error rate of channel, there is always a threat of security control packets such as key exchange being damaged or tampered with. Even if we assume that channel is somewhat reliable, there is no guarantee that communication will also be reliable. Because of the broadcast nature of the wireless media, conflicts and collision in transit are bound to happen. Another feature, multi hop communications may also lead to greater delays or latency and thus real time synchronization[2] is necessary for key exchange.

B. Unmonitored Operations

Being deployed in harsh environments and often left unattended for long time, the sensor nodes become more susceptible towards physical attacks such getting damaged by adversaries, foul weather. Also since the WSN is being managed from a distant place, it's tedious and virtually impossible to find out tampering which may compromise the security of WSN.

Many other issues such as topology also determines the security of WSN and sensor nodes. For example a hierarchical topology with star network and use of repeater may require different levels of security at different levels of hierarchy[3].

III. SECURITY GOALS

In this section, the various security requirements and goals of the security mechanisms will be discussed. Table 1 briefly explains them.

TABLE I. SECURITY GOALS OF WSN

Confidentiality	The sensor node must not leak the sensor data to its neighbors without being permitted to do so[4]. A secure channel, thus, must exist for exchange of sensitive information such as key exchange. Information related to identity of nodes must be in encrypted form[5].
Integrity	It means prevention against the unwanted modifications of sensor transmitted data
Freshness	Data freshness means the data being transmitted is recently gathered by sensor and it's not a mere replay of old data. This is of high importance goal in WSN. For example the shared secret key is destroyed each time a session ends and new keys must be used. Data freshness ensures this.
Secure access	It deals with providing access to services or network only to authorized users
Availability	The network and connection must be available to authorized users all the time. The availability is a fragile issue in WSN because of factors such as single point of failure and additional computation will consume more power
Authentication	The identity of the user accessing the system must be established and verified. Data authentication ensures that data is sent by legitimate user. It is accomplished with use of Message Authentication Key (MAC).
Synchronization	Synchronization is necessary for computing end to end latency. [6] Proposes a secure synchronization for pairwise and group communications.
Others	Apart from the above mentioned goals and requirements, secured localization mechanisms such as Verifiable Multilateration[7] and SeRLoc[8] .

IV. WSN SECURIITY THREATS AND ATTACKS

A. *Physical Attacks*

Being deployed in distant places and away from monitoring location, sensor networks are prone to physical attacks such as deliberate tampering with sensor circuits or destroying the sensors completely, changing the circuit or sensor programming and replacing the sensor with a compromise sensor under the control of malicious user.One such study is being performed in[9].

B. *Evesdropping and Traffic Analysis*

The adversary may find out the frequency at which the sensor node is transmitting data and listens the communication to figure out critical information such as network configuration. Traffic analysis is often conducted in tandem with eavesdropping. The intruder computes the amount of traffic between sensor nodes and extracts which nodes are most critical and performs attack on them.one can also identify which and where the base station is[10].

C. *Denial of Service (DoS) Attacks*

Jamming is a kind of denial of service attack in which the adversary find outs the frequency of transmission and tries to interfere with it. Denial of service attack can also be performed on data link layer by keeping the transmission media busy and constantly leading to collision when a sensor node tries to send data. At network layer, the DoS attack is performed by deliberately dropping the packet instead of forwarding it[11]. At the transport layer, DoS is done by using SYN flooding and opening too many half opened TCP connections to consume enough resources and denying access to legitimate users.

D. *Sybil Attack*

Sybil attack simply means posing as multiple separate identities. Sybil often clouds the efficiency of data aggregation algorithms, routing algorithms resource sharing and allocation mechanisms. [12] Demonstrates Sybil attack specifically in context of sensor networks. For example, in WSN clusters, while deciding for cluster head, Sybil attack can be performed to gain undue advantage in votes.

E. *Node Duplication Attack*

Using this, the adversary attempts to add a sensor node into an existing network by duplicating the ID of an already existing node[13]. Then that duplicated node can be used to misroute the packets or drop critical data packets, affecting the overall performance of the network. Adversary can also try to get his/her hands on cryptographic keys of the sensor network.

V. SECURITY GOALS AND CRYPTOGRAPHIC PARADIGMS

A. *Authentication and Physical and Data Link Layer Security*

The most primitive way to ensure security is to have some kind of authentication mechanism for the network. In applications where data exchanges are less authentication can be accomplished using Access Lists (ACL). ACL is simply a database with list of nodes and privileges granted to them in rule based manner. Whenever a node tries to communicate, the receiver first looks up its ACL for the identity of the sender and if it exists, the communication is done. Since the sensor nodes do not have that much memory to maintain access lists, it is implemented in centralized manner with sink node maintaining the ACL.

For dealing with attacks at physical and data link layer such as eavesdropping, jamming, spread spectrum techniques such as FHSS can be very effective. Since the sender hops onto different frequencies while communicating, it's difficult for attacker to detect the original frequency of communication. An effective approach to tackle traffic analysis attack has been proposed in[10]. Under this method, the packet is forwarded to some other node before sending to sink, making it difficult for intruder to detect the original and clear path.

B. Using Symmetric Key Cryptosystems

Being computationally simple, symmetric key cryptography algorithms are first choice for security in WSN. Algorithms such as DES, 3DES, AES, RC5 have been successfully implemented in sensor networks. But most often used of them is RC5. It is due the reason that RC5 is efficient, computationally simpler, fast, and flexible. AES uses large size look up tables and DES uses extremely large S-box and P-box tables, making them somewhat complex for WSN. Variants of AES-128/192/256 work more efficiently on nodes with higher computation capabilities and is implemented in Counter mode with Cipher Block Chaining- MAC (CBC-MAC).

C. Security Network Encryption Protocol (SNEP)

SNEP[14] provides security for two kinds of communications occurring in sensor networks: from sink node to any sensor node and from a sensor node to sink. It does not provide security for broadcasts. It incorporates Authentication and Integrity by using Message Authentication codes, privacy by using RC5 algorithm in counter mode and data freshness by using a counter. It has very little memory space requirements and minimal computational overhead.

D. Key Establishment Algorithms

A pre distribution key establishment protocol has been proposed in[15]. It is based upon probabilistic approach to key sharing. Each sensor node in the network has a key ring containing randomly chosen keys from a specified key pool. It, however fails to scale efficiently for large sensor networks.

LEAP[16] is another key establishment protocol that relies on multi keying mechanism. Four types are keys are used and each sensor is initially loaded with a key from which other keys can be extracted. Different key is used for different type of communication. The initial key is deleted after using it.

PIKE[17], yet another key establishment protocol employs trust based approach. A secret key between two communicating sensor nodes is established upon mutual trust of a third node. This third node will share the secret key with both the communicating nodes. Over the years, several other key establishment approaches have been proposed which rely on energy differences, capabilities of sink node and other normal sensor nodes. Various certificate based mechanisms have also been promulgated, but they put additional burden on sensor nodes to create and verify digital signatures.

E. Using Asymmetric Key Cryptosystems

Gura et al. in[18] compared the operations of RSA and Elliptic Curve Cryptosystems on 8 bit CPUs and found that the ECC has a significant edge over RSA in terms of efficiency. RSA was later successfully implemented in Berkeley and MICA2 motes[19]. *Tiny PK*[20] incorporates authentication and key management in resource limited sensor networks. *TinySec* [21]uses Diffie Hellman key exchange protocol and RSA on Berkeley motes. Several other public key cryptosystems such as Diffie Hellman over elliptic curves have been proposed which work efficiently for sensor networks.

F. Secured Routing Protocols

In past, more research has been done on designing energy efficient protocols for routing and security in router has been somewhat overlooked. Secured routing is an absolute imperative because network layer being unreliable is more susceptible to adversary. Furthermore it is also necessary to secure the exchange packets while routing them as they carry sensitive information such as topology of network. INSENS[22] is an intruder resistant routing protocol. Authors of the protocol make no distinction between external intruder and a malfunctioning node which implicitly acts as an intruder as it can maliciously drop packets. The idea in this approach is to send the multiple copies of data packets via different routes ensuring that at least one will successfully reach the destination.

µTESLA[14] defines a public key cryptosystem incorporating a key distribution mechanism. Sender generates a secret key and broadcasts the message along with key. Sender defers disclosure of the key and till then receiving nodes buffer the incoming packets. After the sender discloses the key, receiver can authenticate the message. Multi-level key can also be used.

TRANS[23] is an advancement to µTESLA. It is used in centralized, loosely time coupled and synchronized networks. It is also a public key cryptosystem. TRANS ensures that data packet is sent along a route that only has trusted and location aware sensor nodes. Sink node broadcasts the encrypted message and trusted node having secret key can decrypt it. The trusted location aware node then encrypts the message, appends its location and forwards it to the next hop. When the packet reaches destination, it is authenticated using MAC. Any reply to the message can be sent along the same secured and trusted route.

Another attack in routing called wormhole attack[24] in which the adversary node tunnels the packet with the help of other malicious node, can be prevented with the use of directional antennas[25]. But this approach is cost-ineffective when employed to large scale sensor networks. Sybil attack can be avoided using validation strategies in which, it is ensured that every participating node in sensor holds only one identity. Validation can be envisaged using direct or indirect approach. In direct scheme, a trusted node explicitly tests the identity of the joining sensor node is valid or not. While in indirect approach, trusted node simply endorses the identity of the node.

G. Secured and Verifiable Data Aggregation

Secure data aggregation is another security aspect to pay heed to. Sensor networks deal with large volume of raw data and thus need aggregators which can process that raw data to generate some meaningful information. Various techniques for

aggregation have been proposed such as clustering[26]. Malice in aggregation can come in form of a compromised aggregator. If such aggregator is compromised then the entire volume of data forwarded to base or sink becomes corrupted. Denial of service also becomes prominent in such scenarios. In[27], authors propose a secure aggregation technique which uses multiple Message authentication codes in the route from aggregator node to sink. If any of these MAC fails to be authenticated, packet is dropped. Secured Localization [28] [29] [30] techniques are also an inherent requirement for many applications such as body area networks and RFID based location identification and verification.

VI. Intrusion Detection In Sensor Networks

Use of cryptographic algorithms and techniques secures the network from external adversaries and does too little to tackle internal malicious node, for example, what if any internal malicious node has got hold of other's secret keys. Therefore robust intrusion detection system need to be employed in the network. IDS can be either host oriented or network oriented[31]. A host oriented intrusion detection system operates on underlying architecture of the host such as operating system audits, logs etc. A network oriented IDS works on the incoming data packets in the network.
More advanced techniques such as signature, specification and anomaly oriented IDS can be used for multi-layered network architecture.

Albers et al. proposed a Local Intrusion Detection System (LIDS)[32], in which intrusion detection is performed at each sensor node locally. Each node and its located LIDS work in a collaborative manner and exchange control packets and intruder alerts to accomplish intrusion detection in entire network. The core architecture of LIDS is demonstrated in following figure Fig 1:

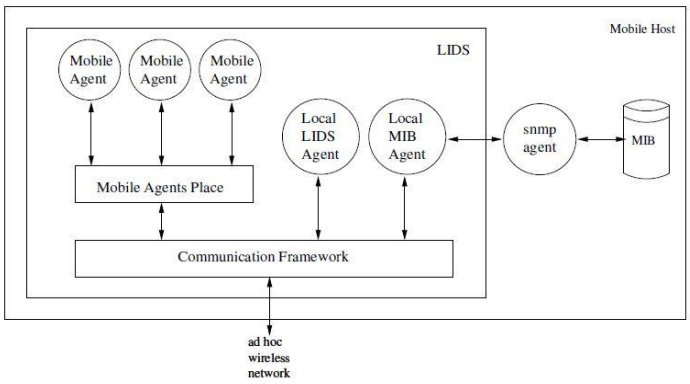

Fig 1. Intrusion detection system

Each sensor node has Simple Network Management Protocol (SNMP) configured on its mobile agent. Management Information Base (MIB) contains various variables and acts as an interface between SNMP agent and communication framework. Mobile agents gather and process intrusion alerts from other hosts and sends intruder alerts to other nodes. For detecting the intrusions, the authors have used SNMP audits.

VII. Conclusion

It is often erroneous to think that same kind of security can be applied to sensor networks as those applied to traditional wireless networks. The implicit limitations of sensor networks, as mentioned in this paper, makes security a tremendous challenge in context of sensor networks. The objective should be to design a security mechanism that scales well with the inherent limitations of WSN. Apart from that the focus should not only be on securing the communication and messages sent, but rather it should also focus on secured routing protocols, secure localization techniques, group management protocols, secured data aggregation, broadcasting and multicasting paradigms. The easement of Internet of Things applications has led to exponential growth in use of ad hoc sensor networks, thus the task of achieving security assumes more significance than ever.

REFERENCES

[1] B. J. M. D. W. Carman, P. S. Krus, "Constraints and approaches for distributed sensor network security.," 2000.

[2] Tian He, J. A. Stankovic, C. Lu, and T. F. Abdelzaher, "SPEED: a stateless protocol for real-time communication in sensor networks," *23rd Int. Conf. Distrib. Comput. Syst. 2003. Proceedings.*, pp. 46–55, 2003.

[3] N. R. Prasad and M. Alam, "Security framework for wireless sensor networks," *Wirel. Pers. Commun.*, vol. 37, no. 3–4, pp. 455–469, 2006.

[4] D. Carman, P. Kruus, and B. Matt, "Constraints and approaches for distributed sensor network security (final)," *DARPA Proj. Rep.*, pp. 1–139, 2000.

[5] A. Perrig, R. Szewczyk, J. D. Tygar, V. Wen, and D. E. Culler, "SPINS: Security protocols for sensor networks," *Wirel. Networks*, vol. 8, no. 5, pp. 521–534, 2002.

[6] S. Ganeriwal, S. Capkun, C.-C. Han, and M. B. Srivastava, "Secure time synchronization service for sensor networks," in *Proceedings of the 4th ACM workshop on Wireless security - WiSe '05*, 2005, p. 97.

[7] S. Čapkun, "Secure positioning in wireless networks," *IEEE J. Sel. Areas Commun.*, vol. 24, no. 2, pp. 221–232, 2006.

[8] L. Lazos and R. Poovendran, "SeRLoc: Secure Range-Independent Localization for Wireless Sensor Networks," *Netw. Secur.*, pp. 21–30, 2004.

[9] W. Gu, X. Wang, S. Chellappan, D. Xuan, and T. H. Lai, "Defending against search-based physical attacks in sensor networks," in *2nd IEEE International Conference on Mobile Ad-hoc and Sensor Systems, MASS 2005*, 2005, vol. 2005, pp. 520–527.

[10] R. Han and S. Mishra, "Countermeasures Against Traffic Analysis Attacks in Wireless Sensor Networks," *First Int. Conf. Secur. Priv. Emerg. Areas Commun. Networks*, pp. 113–126, 2005.

[11] D. R. Raymond and S. F. Midkiff, "Denial-of-service in wireless sensor networks: Attacks and defenses," *IEEE Pervasive Comput.*, vol. 7, no. 1, pp. 74–81, 2008.

[12] J. Newsome, E. Shi, D. Song, and A. Perrig, "The sybil attack in sensor networks: analysis & defenses," *Proc. third Int. Symp. Inf. Process. Sens. networks IPSN04*, pp. 259–268, 2004.

[13] and V. G. B. Parno, A. Perrig, "Distributed detection of node replication attacks in sensor networks.," in *In Proceedings of IEEE Symposium on Security and Privacy*, 2005.

[14] A. Perrig *et al.*, "SPINS : Security Protocols for Sensor Networks SPINS : Security Protocols for Sensor Networks," *Wirel. Networks*,

vol. 8, pp. 521–534, 2002.

[15] L. Eschenauer and V. D. Gligor, “A key-management scheme for distributed sensor networks,” *Proc. 9th ACM Conf. Comput. Commun. Secur.*, pp. 41–47, 2002.

[16] S. S. and S. J. S. Zhu, “LEAP: efficient security mechanism for large scale distributed sensor networks,” in *Proceedings of 10th ACM conference on Computer and Communication security*, 2003.

[17] H. Chan and A. Perrig, “PIKE: Peer Intermediaries for Key Establishment in Sensor Networks,” *Ieee Infocom*, vol. 1, no. Cc, pp. 524–535, 2005.

[18] N. Gura, A. Patel, A. Wander, H. Eberle, and S. C. Shantz, “Comparing elliptic curve cryptography and RSA on 8-bit CPUs,” *Lect. notes Comput. Sci.*, pp. 119–132, 2004.

[19] J. Hill, R. Szewczyk, A. Woo, S. Hollar, D. Culler, and K. Pister, “System architecture directions for networked sensors,” *ACM SIGOPS Oper. Syst. Rev.*, vol. 34, no. 5, pp. 93–104, 2000.

[20] R. Watro, D. Kong, S.-F. Cuti, C. Gardiner, C. Lynn, and P. Kruus, “TinyPK: Securing Sensor Networks with Public Key Technology,” *2nd Work. Secur. Ad Hoc Sens. Networks SASN'04*, no. October, pp. 59–64, 2004.

[21] C. Karlof, N. Sastry, and D. Wagner, “TinySec: a link layer security architecture for wireless sensor networks,” *Security*, vol. 3, pp. 162–175, 2004.

[22] and S. M. J. Deng, R. Han, “INSENS: intrusion-tolerant routing in wireless sensor networks,” 2002.

[23] S. Tanachaiwiwat, P. Dave, R. Bhindwale, and A. Helmy, “Secure Locations: Routing on Trust and Isolating Compromised Sensors in Location-Aware Sensor Networks,” *SenSys '03*, p. 2, 2003.

[24] and D. B. J. Y. Hu, A. Perrig, “Packet leashes: a defense against wormhole attacks in wireless networks.,” in *In INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications Societies*, 2003, pp. 1976–1986.

[25] L. Hu and D. Evans, “Using Directional Antennas to Prevent Wormhole Attacks,” *Netw. Distrib. Syst. Symp. NDSS*, no. February, pp. 1–11, 2004.

[26] D. Estrin, J. Heidemann, S. Kumar, and M. Rey, “Next Century Challenges: Scalable Coordination in Sensor Networks,” *Proc. ACM/IEEE Int. Conf. Mob. Comput. Netw.*, no. Section 4, pp. 263–270, 1999.

[27] Z. Yu and Y. Guan, “A dynamic en-route filtering scheme for data reporting in wireless sensor networks,” *IEEE/ACM Trans. Netw.*, vol. 18, no. 1, pp. 150–163, 2010.

[28] A. Kumar and B. Saini, “A Sugeno-Mamdani Fuzzy System Based Soft Computing Approach Towards Sensor Node Localization with Optimization", In: Bhattacharyya P., Sastry H., Marriboyina V., Sharma R. (eds) Smart and Innovative Trends in Next Generation Computing Technologies. NGCT 2017. Communications in Computer and Information Science, vol. 828. pp 40-55, Springer, Singapore..

[29] A. Kumar and D. Prashar, “A Novel Approach for Node Localization in Wireless Sensor Networks", In: Singh R., Choudhury S., Gehlot A. (eds) Intelligent Communication, Control and Devices. Advances in Intelligent Systems and Computing, vol. 624. pp 419-428, Springer, Singapore

[30] A. Kumar, “A Hybrid Fuzzy System Based Cooperative Scalable and Secured Localization Scheme for Wireless Sensor Networks,” *Int. J. Wirel. Mob. Networks*, vol. 10, no. 3, pp. 51–68, Jun. 2018.

[31] P. Brutch and C. Ko, “Challenges in intrusion detection for wireless ad-hoc networks,” *Applications and the Internet Workshops, 2003. Proceedings. 2003 Symposium on*. pp. 368–373, 2003.

[32] P. Albers, O. Camp, and J. Percher, “Security in ad hoc networks: a general intrusion detection architecture enhancing trust based approaches,” *Proc. First Int. Work. Wirel. Inf. Syst.*, pp. 1–12, 2002.