Security Analysis for WSN Based on Cryptographic Method

M.D.S.Nandini
Assistant Professor /ECE
SNS college of Engineering
Coimbatore, India.

Anitha.S.M
UG scholar /ECE
SNS college of Engineering
Coimbatore, India

Jeevhanprithiv.N
UG scholar/ECE
SNS college of Engineering
Coimbatore, India.

Abstract: **This paper describes security solutions for collecting and processing data in Wireless Sensor Networks (WSNs). It includes an overview on security and reliability challenges for WSNs based on the cryptographic techniques. Analysis of securities attacks which includes Passive Attack, Active Attack, Distributed Attack, Insider Attack, Buffer overflow, Exploit attack, Close-in Attack, Phishing Attack, Password attack, Hijack attack and Spoof attack**

I. INTRODUCTION

Wireless Sensor Networks (WSNs) use tiny, inexpensive sensor nodes with several distinguishing characteristics: they have very low processing power and radio ranges, permit very low energy consumption and perform limited and specific monitoring and sensing functions. Several such wireless sensors in a region self-organize and form a WSN. Information based on sensed data can be used in agriculture and livestock,assisted driving or even in providing security at home or in public places. A key requirement from both the technological and commercial point of view is to provide adequate security capabilities. Fulfilling privacy and security requirements in an appropriate architecture for WSNs offering pervasive services is essential for user acceptance.

II. RELATED WORK

One of the advantages of wireless sensors networks (WSNs) is their ability to operate unattended in harsh environments in which contemporary human-in-the-loop monitoring schemes are risky, inefficient and sometimes infeasible. Therefore, sensors are expected to be deployed randomly in the area of interest by a relatively uncontrolled means,[1] e.g. dropped by a helicopter, and to collectively form a network in an ad-hoc manner. Given the vast area to be covered, the short lifespan of the battery-operated sensors and the possibility of having damaged nodes during deployment, large population of sensors are expected in most WSNs applications. It is envisioned that hundreds or even thousands of sensor nodes will be involved. Designing and operating such large size network would require scalable architectural and management strategies

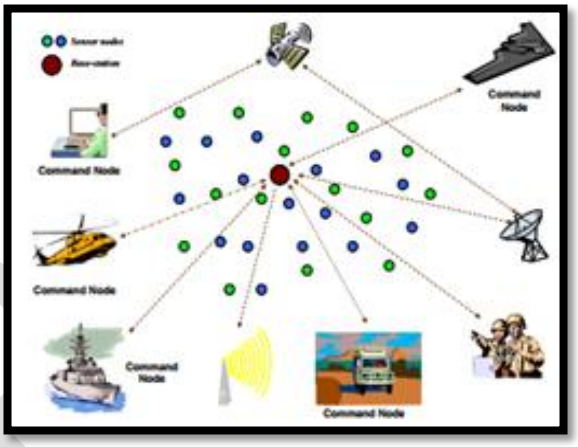


Fig1. An articulation of sample WSN architecture for a military application.

Mutual authentication and access control (MAAC)

The first step is to establish key between nodes. To meet scalability requirements for a large number of sensor nodes, we propose a public key management scheme based on Elliptic Curve Cryptography (ECC). Compared to symmetric key cryptography, ECC is more scalable, requires lesser memory for storing keys, introduces low communication overhead, it is easy to deploy and more secure for sending sensitive data to medical server.

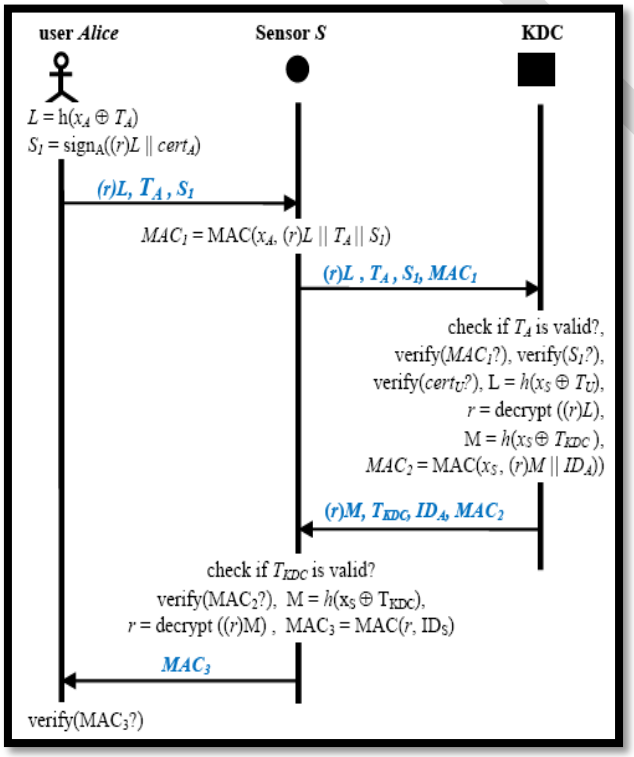
1. Key Establishment

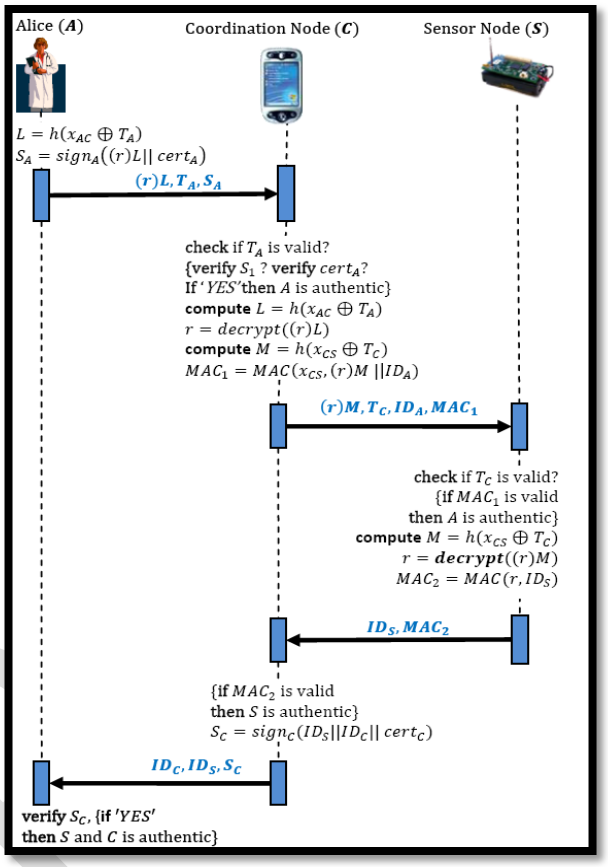
Initially, it selects a particular elliptic curve over a finite field GF(p) (where p is a prime) and publishes a base point with a large order (where is also a prime). It picks a random number x€ GF(p) as a private key, and publishes its corresponding public key Q= x * P . It also generates a random number x_i € GF(p) as a private key for a sensor and generates a corresponding public key Q_i= x * P . The key-pair is then loaded to A. For each node in CN and BN layers, it generates this key-pair $\{x_i, Q_i\}$ based on the base by itself .since it is more powerful than sensor node. After this step, every node in the network has an ECC key-pair which will be used to establish secret (symmetric) key for secure communication. The proposed scheme is based on

Elliptic Curve Diffie- Hellman (ECDH) to establish a shared secret key between two nodes.

2. Authentication

MAAC is enhanced from previous work ENABLE to meet security requirements in healthcare environment. We consider a situation that a medical professional or a healthcare server
(generally called *Alice*, or) wants to access data from a particular sensor, a group of sensors, or data on the coordination node. For proposed MAAC, *Alice* computes secrete key L with accessing list and current time stamp, after that it encrypts the value r with key L i.e. r(L) and computes signature S_A with certificate produced by A. These combinations are send it to coordination node C, it verifies the T_A ,S_A ,L from A. if all the combinations are verified from A ,it will authenticate to C ,after that it will computes the secrete key M and it gives message authentication code(MAC_1) with encrypting the value r with key M i.e. r(M). The combinations produced by C are send to Sensor node S, immediately it will checks the time stamp of C are valid or not, and also checks MAC_1 produced by C is valid or not, if it is valid A is authenticate to S and it computes M and produces new MAC_2 .All these computed value are given to C for verification. In C node checks the validity of MAC_2, if valid then S_C is authenticated to C and produces signature with certificate. Finally from A verifies S_C if it is valid then S and C are authenticated , so we have to send a sensitive information of the patients record to medical practioner.





III. SECURITY ANALYSIS

Note that security level of the proposed protocol deponds on the security level of ECC, message authentication code (MAC), and encryption algorithm. Those have been proven secure in this paper.

A. It provides mutual authentication

node verifies the signature *SA*. If *SA* is valid, then the user is authentic to because only *Alice* can generate the signature *SA* by his private key. Consequently, the user is also authentic to sensor *S* because *S* trusts C. On the other hand, only *S* shares the secret key x_{cs} with C .it means that only *S* can decrypt (*r*)M (where M=h(x_{CS} +T_C). So if S can achieve r from (r)M to build (MAC_2 = MAC (r, ID_A) then is authentic to the user. The mutual authentication is provided through trust relations between Alice –C and S – C.

B. It can defend against replay attacks

The adversary can intercept the message sent out from *Alice* or from the sensor *S* .However, both cases are not possible in MAAC because can easily detect by verifying timestamp *TA*. If *TA* is older than a predefined threshold, it is invalid because it has been used for previous authentication. If *TA* was changed, then S_A = $sign_A$((r)L||$cert_A$)) where L=h(x_{AC} +T_A)

C. It can mitigate DoS attack

Upon receiving the message from C, sensor node first checks the validity of timestamp . If it is not valid, then S discards the message. Otherwise, it computes a MAC value to compare with received. A message authentication code (MAC) generated.The proposed scheme significantly reduces *DoS* compared to previews schemes

	Requirement	Range
Operating space	In, on or around the body	Up to 3m
Data rate	scalable	Up to 10mbps
Bands	Unlicensed, medical approved bands	ISM
Duty cycle	scalable	100%
Power consumption	scalable	Up to 40mw
Security	High	Authentication, privacy, encryption
saftey	High	Meet regulation requirement
Topology	Multiple links	No signal point failure
Network setup	required	secure
Location information	Desirable	Localization within a radius

Table 1 REQUIREMENT USED FOR PROPOSED METHOD

Key	128bits
Signal strength	16 bits
Maximum distance transmitted	3m
Number of nodes	25-50

Parameter	Value
Area	100m*100m
Simulation time	5 minutes
Transmission range	10meter
Radio Propagation Model	Two Ray Model
Channel Type	Wireless Channel
Network Interface Model	Phy/ Wireless Phy/IEEE 802.15.4
MAC Model	Mac/ IEEE 802.15.4
Interface Queue Type	Drop tail
energy model	micaz
Antenna model	Omni antenna
Maximum Packet	50
No of Mobile Nodes	10-50
Routing Protocol	AODV
each item size	64 bytes
Operating frequency	2.4 GHz

Table 2 PARAMETERS USED FOR PROPOSED METHOD

IV. TYPES OF ATTACK

Classes of attack might include passive monitoring of communications, active network attacks, close-in attacks, exploitation by insiders, and attacks through the service provider. Information systems and networks offer attractive targets and should be resistant to attack from the full range of threat agents, from hackers to nation-states. A system must be able to limit damage and recover rapidly when attacks occur.

There are five types of attack:

Passive Attack

A **passive attack** monitors unencrypted traffic and looks for clear-text passwords and sensitive information that can be used in other types of attacks. **Passive attacks** include traffic analysis, monitoring of unprotected communications, decrypting weakly encrypted traffic, and capturing authentication information such as passwords. Passive interception of network operations enables adversaries to see upcoming actions. Passive attacks result in the disclosure of information or data files to an attacker without the consent or knowledge of the user.

Active Attack

In an **active attack,** the attacker tries to bypass or break into secured systems. This can be done through stealth, viruses, worms, or Trojan horses. Active attacks include attempts to circumvent or break protection features, to introduce malicious code, and to steal or modify information. These attacks are mounted against a network backbone, exploit information in transit, electronically penetrate an enclave, or attack an authorized remote user during an attempt to connect to an enclave. Active attacks result in the disclosure or dissemination of data files, DoS, or modification of data.

Distributed Attack

A **distributed attack** requires that the adversary introduce code, such as a Trojan horse or back-door program, to a "trusted" component or software that will later be distributed to many other companies and users Distribution attacks focus on the malicious modification of hardware or software at the factory or during distribution. These attacks introduce malicious code such as a back door to a product to gain unauthorized access to information or to a system function at a later date.

Insider Attack

An **insider attack** involves someone from the inside, such as a disgruntled employee, attacking the network Insider attacks can be malicious or no malicious. Malicious insiders intentionally eavesdrop, steal, or damage information; use information in a fraudulent manner; or deny access to other authorized users. No malicious attacks typically result from carelessness, lack of knowledge, or intentional circumvention of security for such reasons as performing a task

Close-in Attack

A **close-in attack** involves someone attempting to get physically close to network components, data, and systems in order to learn more about a network Close-in attacks consist of regular individuals attaining close physical proximity to networks, systems, or facilities for the purpose of modifying, gathering, or denying access to information. Close physical proximity is achieved through surreptitious entry into the network, open access, or both.

One popular form of close in attack is **social engineering** in a social engineering attack, the attacker compromises the network or system through social interaction with a person, through an e-mail message or phone. Various tricks can be used by the individual to revealing information about the security of company. The information that the victim reveals to the hacker would most likely be used in a subsequent attack to gain unauthorized access to a system or network.

Phishing Attack

In phishing attack the hacker creates a fake web site that looks exactly like a popular site such as the SBI bank or paypal. The phishing part of the attack is that the hacker then sends an e-mail message trying to trick the user into clicking a link that leads to the fake site. When the user attempts to log on with their account information, the hacker records the username and password and then tries that information on the real site.

Hijack attack

Hijack attack In a hijack attack, a hacker takes over a session between you and another individual and disconnects the other individual from the communication. You still believe that you are talking to the original party and may send private information to the hacker by accident.

Spoof attack

Spoof attack In a spoof attack, the hacker modifies the source address of the packets he or she is sending so that they appear to be coming from someone else. This may be an attempt to bypass your firewall rules.

Buffer overflow

Buffer overflow A buffer overflow attack is when the attacker sends more data to an application than is expected. A buffer overflow attack usually results in the attacker gaining administrative access to the system in a ommand prompt or shell.

Exploit attack

Exploit attack In this type of attack, the attacker knows of a security problem within an operating system or a piece of software and leverages that knowledge by exploiting the vulnerability.

Password attack

Password attack An attacker tries to crack the passwords stored in a network account database or a password-protected file. There are three major types of password attacks: a dictionary attack, a brute-force attack, and a hybrid attack. A dictionary attack uses a word list file, which is a list of potential passwords. A brute-force attack is when the attacker tries every possible combination of characters.

Scheme	Message content	Message size	Total Energy	Authentication
DCF	**Solicitation:**<ID, CERT> **Reply:**<ID, CERT>	$s = \|ID\| + \|Cert\|$ $y = s$	$T = sLEt + sQLEr + yEt(N - L) + yEr(N - L)$	-
DCF-KDC	**Key Distribution** **Request:**<ID,Q(ID),MAC> **Reply:**<ID,Key>	$r = \|ID\| + Q\|ID\| + \|MAC\|$ $y = \|ID\| + \|Key\|$	$T = rLEt + y(Q+1)LEr + Edprot$	-
ENABLE	$L = h(xA + TA)$ $S1 = signA((r)L \|\| certA)$	$M = h(Xs + TKDC)$, $MAC2 = MAC(xS, (r)M \|\| IDA))$	MAC3 = MAC(r, IDS)	-
MAAC	$L = h(xA + TA)$ $S1 = signA((r)L \|\| certA)$	$M = h(Xs + TKDC)$, $MAC2 = MAC(xS, (r)M \|\| IDA))$	$M = h(xS + TKDC)$, MAC3 = MAC(r, IDS)	$S_C = sign_C (ID_S \|\| ID_C \|\| cert_C)$
FPWK	-	1 COMPROMISED KEY IN WORKING PHASE	X NODES COMPROMISED IN THE WORKING PHASE	-
	$\frac{2}{n^2}$	$\frac{2}{n}$	0	1
EG	-	$\frac{1}{p}$	$\frac{r}{p}$	-
LEAP+	-	$\frac{2}{vn}$	$\frac{2}{n}$	-
SKKE		$\frac{2}{vn}$	$\frac{2}{n}$	-

V. CONCLUSION

We described security and reliability challenges for WSNs.we analyze security attacks in WSN applications. Our scheme have better performance in terms of key storage, number of operations performed and number of messages exchanged during key establishment based on the cryptographic methods.

REFERENCES

[1]. Mani B. Srivastava Curt Schurgers. Energy efficient routing in wireless sensor networks. MILCOM'01, pages 357–361, October 28-31 2001.

[2]. I. Matta V. Erramilli and A. Bestavros. On the interaction between data aggregation and topology control in wireless sensor networks. In Proc. of SECON,, pages 557–565,, Oct 2004.

[3]. S. Bandyopadhyay and E. J. Coyle. An energy efficient hierarchical clustering algorithm for wireless sensor networks. In Proceedings of the IEEE Conference on Computer Communications (INFOCOM), 2003.

[4]. S. Ghiasi, A. Srivastava, X. Yang, and M. Sarrafzadeh. Optimal energy aware clustering in sensor networks. Sensors, 2:258–259, 2002.

[5]. Anathan P. Chandraskan Wendi B. Heinzelman and Hari Blakrisshnan. An application-specific protocol architecture for wireless microsensor networks. IEEE Trans. on Wireless Communications, 1(4):660–670, OCT 2002.

[6]. Konstantinos Kalpakis Koustuv Dasgupta and Parag Namjoshi. An effi- cient clustering-based heuristic for data gathering and aggregation in sensor networks. In IEEE Wireless Communications and Networking Conference, 2003.

[7]. Koustuv Dasgupta Konstantinos Kalpakis and Parag Namjoshi. Maximum lifetime data gathering and aggregation in wireless sensor networks. In IEEE International Conference on Networking, pages 685–696, August 2002.

[8]. Daniel Kofman Ravi Mazumdar Ness Shroff Vivek P. Mhatre, Catherine Rosenberg.

[9]. Nandini.M.D.S, Kiruthika.M "Life Time Balanced Routing Algorithm for Wireless Sensor Networks", IJARCSMS published 2014.

[10]. Nandini.M.D.S ,Sangeetha.K"Energy Based Routing Algorithm Using Spanning Tree For Multicluster Formation In WSN" IJAICT Volume 1, Issue 2, June 2014.