Wireless Sensor Network - Authentication Protocol for Military Surveillance

Varsha Jathar[1] Louella Menezes Mesquita e Colaco[2]
[1]P.G. Student [2]Assistant Professor
[1]Department of Information Technology [2]Department of Computer Engineering
[1,2]Padre Conçeicao College of Engineering, Verna- Goa, India

Abstract— Wireless sensor network are being used widely across various security applications such as monitoring, tracking, surveillance systems and also controlling the areas in military and battlefield. However widely used wireless networks are prone to unique security challenges such as node forgery, denial of service attack, and other hostile network attacks. In military surveillance system an intruder can introduce malicious nodes or manipulate the existing nodes to set up malicious node. To avoid participation of malicious node from joining the sensor network, a security consideration is required in the design of network protocol. Also military applications require multimedia data such as images, text or videos to be transmitted across the network area. In this paper, we propose a security protocol to provide authentication of nodes within the sensor network and perform multimedia transfer between source and destination. When deployed within network a high degree of security is achieved compared to conventional security applications. This paper implements ECC based authentication protocol suitable for military applications using wireless network where security is in demand.

Key words: Multimedia authentication, node security, wireless multimedia security, security protocol, wireless multimedia authentication protocol, source authentication

I. INTRODUCTION

Nowadays Security allows wireless sensor networks to be used with secrecy, reliability and integrity. Without security mechanism, the Wireless Sensor Network (WSN) usage in any application domain may lead to malicious attacks across network. Technological innovation and advancement in today's state-of-art WSN have lower deployment and maintenance cost, last longer and is more rugged. The wireless sensor network consist of sensing nodes which are capable of monitoring parameters and communicating with other nodes over a physical environment for some purpose like monitoring, surveillance, target tracking. The communication among sensor nodes is done using wireless transceivers within their range. Thus sensor nodes also called as motes capture data and transfer this data to a single point called base station or Gateway node.

WSN provided support for communication systems to be used in various navy, military systems using multimedia data objects like still images, audio/video stream, and text files. WSN can be used by military services data processing such as monitoring, tracking the enemies and force protection, catching global parameters. Military services are rapidly growing towards innovative technology with advanced implementation of security protocol at various application levels. Video and audio sensors can be used to enhance and complement existing surveillance systems against crime and attacks [1].

Wireless sensor networks have unique challenges; traditional security techniques used in classical network cannot be applied directly. To make wireless sensor highly viable, sensor devices are limited with their energy, cmputation and communication capabilities. Secondly, sensor nodes are deployed in open accessible areas adding risk of physical damage or attacks. Third, sensor networks are often interacting with physical environments imposing new security issues. Consequently existing security mechanisms are not efficient and new techniques are needed.

There is a basic need to give protection and security confirmations to disseminated sight and sound sensor organizing in applications including military systems and medicinal services observing. Such ensures empower the far reaching selection of such data frameworks, prompting expansive scale societal advantage. To adequately address insurance and unwavering quality.

Authentication Protocol for Military Surveillance issues, secure interchanges and handling must be considered from framework origin. Because of the developing way of broadband sensor frameworks, this gives fruitful exploration ground to proposing more outlook changing methodologies. Assurance issues inside this engineering are investigated; prompting the improvement of open examination issues incorporating secure steering in rising free-space optical sensor arranges and dispersed protection for vision-rich sensor organizing.

II. SYSTEM MODEL

A. Existing System

WSN provided support for communication systems to be used in various navy, military systems using multimedia data objects like still images, audio/video stream, and text files. WSN can be used by military services data processing such as monitoring, tracking the enemies and force protection, catching global parameters. Military services are rapidly growing towards innovative technology with advanced implementation of security protocol at various application levels. Video and audio sensors can be used to enhance and complement existing surveillance systems against crime and attacks.

Recent advances in wireless and electronic technologies have enabled a wide range of applications of multimedia sensor networks in traffic engineering, source target tracking, navy n border security services, and location monitoring, healthcare domains and so on.

The existing authentication protocol have enabled wide range of applications of WMSNs in military sensing, traffic surveillance, target tracking, environmental monitoring etc. Experiments are done in border surveillance and intrusion detection using technology of WSN. Many

public key communication methods are being used such as RSA, Diffie-Hellman, DSA, ECC etc.

The system proposed a distributed authentication scheme in WSN. It is based on self- certified cryptosystem which is changed to use Elliptic curve based method to get the pair wise keys in sensor network. RSA based system involves basically on complexity large integers factoring.

Whiefield Diffie and Martin Hellman introduced the public cryptography called Diffie Hellman key exchange. DH is key exchange and DSA is signature based algorithm which can be combined to perform valid key agreement method, as both exchange of keys and signature algorithm are based on the difficulty of solving discrete problem in the multiplicative group of integers modulo a prime p. Elliptic curve groups were introduced as a substitute for multiplicative groups. For same level of security ECC system can be implemented with much smaller parameters with better performance advantages.

B. Proposed System

The proposed scheme introduces security authentication protocol for deployment of new node in military surveillance systems to perform multimedia data transfer across the nodes. In this protocol we will develop authentication mechanism for nodes using ECC algorithm. The sensor nodes are used to capture data objects such as images, video, audio stream across borders and once the data is captured it is transmitted across network making use of ECC public key communication.

The system extends ECC algorithm and enables multi-hop transmissions across clusters by incorporating selection of authentic sending and receiving nodes. Thus it performs 2 tasks: authentication of nodes and data transfer between source and destination node. The proposed system needs Certificate Authority to issue the certificate to the pre-deployed nodes, for secure data transfer across network and verification of the node with signature is done before session begins for data transfer. Thus performance of the proposed system is evaluated in terms of throughput and packet delay rate. The existing system is enhanced by allowing more security level across multihop wireless network used in military surveillance in which base station is used as certificate authority and Cluster heads are used for routing the data packets from source to destination node and support minimum packet loss with more efficient performance as compared to conventional system.

III. PROPOSED AUTHENTICATION PROTOCOL

A. Wireless Multimedia Sensor Network for Military

Wireless sensor networks have been undergoing a fast growth in upcoming years due to the joint efforts of both academia and industry in developing this technology. Recent WSN's are adopted in a wide range of applications as a better solution able to replace existing wired and wireless systems that are more expensive and hard to set up because of their requirement of high power consumption and cables required for connection of the networks. A reduced set of WSN application include climatic monitoring, structural monitoring of buildings, human tracking, military surveillance and multimedia related applications.

The wireless multimedia sensor networks (WMSNs) development has been mainly fostered by a new generation of low-power and high performance microcontroller able to speed up the processing capabilities of single wireless node, as well as development of new micro cameras and microphones imported from the mobile phone industry [2,3]. Along with classical multimedia applications in which audio and still images and text data can be sent through the networks, pervasive WMSNs consisting of large deployments of camera sensor may support latest Vision base systems. By collecting and analyzing images from the scene, notorious and potentially dangerous activities can be detected, advanced applications based on human activities can be enabled and intelligent services can be provided.

B. Multimedia Content

Multimedia content produces a huge amount of data. The data is compacted by employing compression techniques, such as, MPEG, H.263 and H.264 which can be classified as predictive coding techniques. The video is compressed once by the sender and uncompressed by the receiver. For MPEG technique 3 different frames are defined:
(I, P, B-frames) are defined, wherein:
Intra, or I-frames, serves as the reference for all other frames which also provides reference point for decoding a received video data.

1) Authentication Protocol for Military Surveillance

Predictive-coded, or P-frames, serves to provide an increased rate of compression as compared to the I-frames, P-frame with possibly being 20-70% the size of associated I-frame. Bi-directionally predictive-coded, or B-frames, uses the previous and next I-frame or P-frame as their reference points for motion compensation. B-frames provide further compression. The nodes in a WMSN are able to capture and transmit multimedia content, which can either be a snapshot or streaming content. A snapshot contains data from an event that was triggered in a short time period, e.g. an image. Streaming multimedia content is generated over a longer time period, e.g. video and audio streaming.

Proposed scheme performs 2 tasks Authentication of new nodes using Certificate authority. Data transfer across nodes routing through Cluster Head. During authentication, shared keys are created between neighboring nodes and deployed node to provide secure authentic communication. The scheme is divided into 2 phases

- Initialization/Pre-deployment Phase
- Authentication Phase.

2) Assumptions

The sensor network is non-static, i.e. the sensor nodes are mobile.

- Each sensor node has preset security time stamp.
- Two sensor nodes may have the same Security Time Stamp if they are deployed simultaneously.
- The base station acts as a controller also acts as CA, as highly secure, trustable and has powerful components in terms of energy, memory and computation.
- All the sensor nodes are variable in terms of energy, memory and computation capabilities as multiple type of data can be transmitted which includes text, audio, video and still images.

- The sensor nodes have enough memory to manage with the keying overheads. Due to a wireless medium an opponent can listen to the entire network traffic once the network is compromised.
- Algorithm and Architecture
- The Algorithm states step by step procedure to perform node Authentication .The Architecture defines the Components required in the Design of Authentication Protocol.

3) Algorithm

- Node B" wants to join network so it sends request to certificate authority for certificate and time stamp, here base station considered as certificate authority.
- Certificate Authority provides a certificate with time stamp to "B" to access network and participate in data transfer.
- "B" sends this certificate to its neighbor A for authentication.
- "A" checks the security time stamp by using certificate.
- "A" checks the validity and identification for authentication of "B" by using authority certificate.
- If "B" is authentic node then Exchange the information.
- The Cluster Head routes the data from source to destination node. The network consist of multihop topology wherein cluster Heads are used to route the packets between source and destination nodes.

C. *Architecture of Surveillance system*

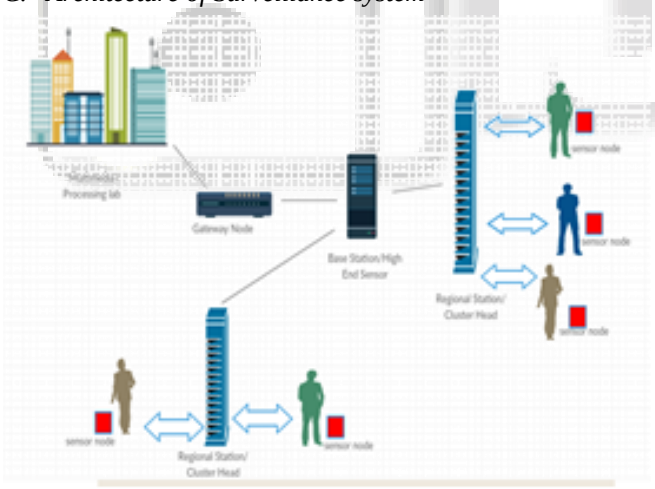

Fig. 1: Surveliance Architecture

D. *Initialization/Pre-deployment Phase*

- Before a sensor network is deployed, the Certificate authority chooses a set of network parameters including which consist of:
- A finite field Fq, where q is a large odd prime of at least 160 bits.
- An elliptic curve E over Fq Ep (a, b) - elliptic curve with parameter a, b and p is prime.
- G: A cyclic group point on elliptic curve whose order is large value n of at least 160 bits.
- The CA's private key k= {1, 2, 3……., n-1}.
- The CA's public key Q=kG and the CA never shares its private key with anyone else. 4.3.1.1 Protocol
- Steps at node B: B first selects private key nb and calculates public key Q=KUb = nb*G B sends its public key to the certificate authority CA. Certificate authority provides certificate to B that include Cb= [Bi, Te, TSb, Ls, KUb]. Cb: certificate of node B issued by CA Bi: identity of B. Te: expiry time of certificate. TSb: security time stamp assigned to B to enter network Kub: public key of B. B sends this message to A.
- Node A checks the validity of security time stamp and identifies node B. Steps at Node A A first compare B's security time stamp TSb With its own security time stamp TSa. If TSb >= TSa then node B might be a new node.
- To authenticate a new node A proceed to verify node B is a new node by comparing TSb with its current time t. If TSb is out of date {TSb – t} > LSb node A simply drop the message.

E. *Multihop Wireless Networks*

Multi-hop wireless networks utilize multiple wireless nodes to provide coverage to an outsized space by forwarding and receiving knowledge wirelessly between the nodes. However, multi-hop networks consist of "hot spots" areas in the network where multiple wireless transmissions will interfere with each other. This limits how quickly the network will transfer knowledge, because the nodes have to move transmitted knowledge at these full points.

Data will be transmitted at low power over short distances, which limits the degree of interference with alternative nodes. But this approach suggests that the information might get to be transmitted through several nodes before reaching its final destination. Two categories: Relay: Tree based mostly is the base station Broadband topology, one end of the path transmission Wireless research laboratory, dedicated carrier owned infrastructure.

IV. RESULTS AND CONCLUSION

A. *Results*

The analysis shows that system achieves maximum throughput providing efficient transmission data rate. Throughput is the rate at which successful data transfer takes place across the network.

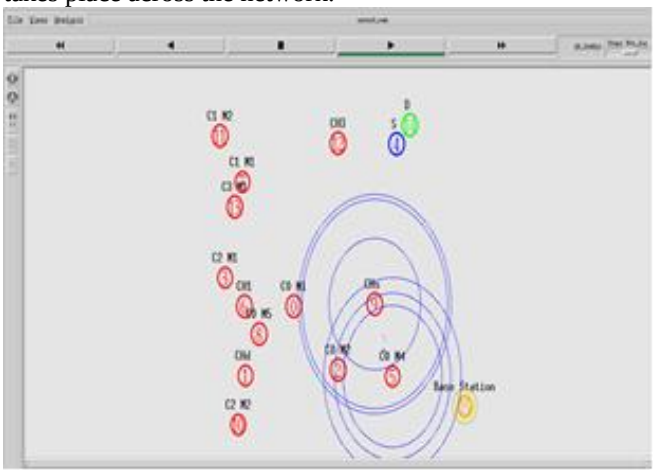

Fig. 2: Cluster and node scenario

The proposed system achieves higher security level as compared to existing ones, since we are using ECC curve which are complex in nature to generate original curves.

However Energy consumption is not considered much, as huge amount of computation is involved and only better security level is provided for data sensitive applications.

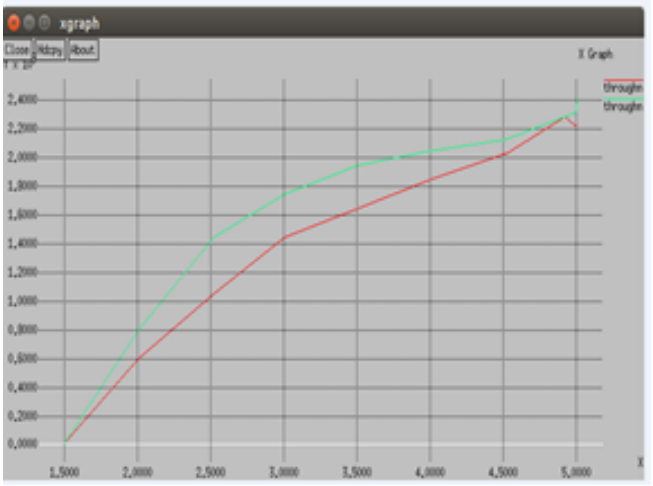

Fig. 3: Throughput

V. CONCLUSION

This project proposes an Authentication Protocol using wireless sensor network designed for military surveillance system. The Protocol allows authentication of sensor nodes which are left in unattended open environment using Certificate, pre-deployment of sensor nodes is essential as parameters needed to generate the certificate. The certificate is generated using ECC based technique in which public and private keys are used to invoke certificate for secure data transfer. The data transfer includes any media transfer like images, videos, text etc depending on hardware configuration of the sensor nodes deployed. The system consist of multi-hop topology wherein Base station serves as central controller with additional regional stations implemented as Cluster heads to provide certificate to members of the clusters. The Protocol focuses on security level then energy consumption as ECC provides higher security levels with reduced key size and number of bits as compared to RSA. Thus system can be considered more secure used across open environment where sensor nodes are deployed for the purpose of data monitoring in critical applications.

REFERENCES

[1] Perrig, R. Szewczyk, J.D. Tygar, V. Wen, D.E. Culler, SPINS: Security protocols for sensor networks, Wireless Networks 8 (September) (2002) 521–534.
[2] Karlof, N. Sastry, D. Wagner, TinySec: a link layer se-curity architecture for wireless sensor networks, in: The Second ACM Conference on Embedded Networked Sen-sor Systems (SensSys'04), Baltimore, Maryland, Novem-ber 2004.
[3] L. Eschenauer, V. Gligor, A key management scheme for distributed sensor networks, in: The Proceedings of the 9th ACM Conference on Computer and Communications Se-curity (CCS'02), Washington DC, 2002.
[4] Haowen Chan, Adrian Perrig, Dawn Song, Random key predistribution schemes for sensor networks, in: Proceed-ings of the 2003 IEEE Symposium on Security and Priva-cy (S&P'03), 11–14 May 2003, p. 197.
[5] Cano, M.D., R. Toledo-Valera and F. Cerdan, 2007. A certification authority for elliptic curve X.509v3 certificates. Proceedings of the 3rd International Conference on Networking and Services, JUN. 1925, IEEE Xplore Press, Athens, pp: 49-49. DOI: 10.1109/ICNS.2007.3
[6] Cao, L.C., 2011. Improving security of SET Protocol based on ECC. Proceedings of the International Conference on Web Information Systems and Mining, Sept. 24-25, Taiyuan, China, Springer Berlin Heidelberg, pp: 234-241. DOI: 10.1007/9783-642-23971-7_31
[7] Dou, B., C.H. Chen, H. Zhang and C. Xu, 2012. Identity based sequential aggregate signature scheme based on RSA. Int. J. Innov. Comput. Inform. Control, 8: 6401-6413.
[8] Muazzam A. Khan, Ghalib A. Shah, Muhammad Sher (2011), "Challenges for Security in Wireless sensor Networks (WSNs)", World Academy of Science, Engineering and Technology
[9] Shio Kumar Singh, M P Singh, D K Singh (2011), "A Survey on Network Security and Attack Defense Mechanism for WSN", Internal Journal of Computer and Technology
[10] G. Padmavathi, D. Shanmugapriya (2009), "A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks", International Journal of Computer Science and Information Security, Vol. 4, No. 1 & 2.
[11] Prajeet Sharma, Niresh Sharma, Rajdeep Singh (2012), "A Secure Intrusion detection system against DDOS attack in Wireless
[12] W. Zhang, N. Subramanian, and G. Wang, "Lightweight and compromiseresilient message authentication in sensor networks," in IEEE INFOCOM, Phoenix, AZ., April 15-17 2008.
[13] M. Albrecht, C. Gentry, S. Halevi, and J. Katz, "Attacking crypto graphic schemes based on "perturbation polynomials"," Cryptology ePrint Archive, Report 2009/098, 2009.
[14] http://waset.org/publications/4180/authentication-protocol-for-wireless-sensor-networks
[15] L. Eschenauer, V. Gligor, A key management scheme for distributed sensor networks, in: The Proceedings of the 9th ACM Conference on Computer and Communications Se-curity (CCS'02), Washington DC, 2002.
[16] W. Du, J. Deng, Y.S. Han, P.K.Varshney, A pairwise key predistribution scheme for wireless sensor networks, in: The Proceedings of the 10th ACM Conference on Com-puter and Communications Security (CCS'03), Washing-ton, DC, 27– 30 October 2003.
[17] Liu, P. Ning, Establishing pairwise keys in distributed sensor networks, in: The Proceedings of the 10th ACM Conference on Computer and Communications Security (CCS'03), Washington, DC, 2003.

