Group Security Model in Wireless Sensor Network using Identity Based Cryptographic Scheme

Asha A[1], Hussana Johar[2], Dr B R Sujatha[3]

[1] *M.Tech Student, Department of ECE, GSSSIETW, Mysuru, Karnataka, India*
[2] *Assistant Professor, Department of TC, GSSSIETW, Mysuru, Karnataka, India*
[3] *Associate Professor, Department of ECE, MCE, Hassan, Karnataka, India*

Abstract - Wireless Sensor Networks have become highly significant in modern technological solutions. They typically comprise of sensor nodes that operate autonomously to gather and transmit data to monitoring and management systems. The applicability of sensor networks now ranges from environment observations to health care management and from infrastructure monitoring to home automation.

This paper explores an approach that provides group security by using an approach of Identity based Cryptography (IBC) schemes. Two specific goals that are addressed in this work includes: (i) approach to authenticate sensors associated to a group with a group controller (ii) method to mutually authenticate sensor group members.

Keywords: wireless sensor Network, security, authentication, cryptography.

1. INTRODUCTION

As deployment of sensor based networks become pragmatic, where in sensor nodes equipped with communication capabilities. Communication capabilities become the key source for collection of various application data in many contemporary technological solutions. The approaches to adoption of sensors are largely categorized into two models – autonomous and group. The autonomous approach of sensing typically consists of nodes that communicate with a data sink or store. This is typically a one-to-one communication. In group model, the sensor nodes that from the group would have some common characteristics like either they produce the same type of data or is controlled by a common authority called group controller. In such cases the communication pattern is one-to-many or many-to-one. For example, a group controller communicates a command message to all nodes in a particular group or each sensor node in the group producing the data to the group controller, a sink to all nodes in the group. One of the classic examples of group model is sensor networks is the command and control of multiple sensors mounted on the arm of a robot, set of sensors installed around a perimeter that produce data to a central command application and so on.

Given the limited and constrained traits of nodes in Sensor Group, security approach for group model not only requires the same level of security and protection as non-constrained node but also at much lower computational cost due the low power nature of these devices. Approaches to group security are constant area of research both in academia and industry.

One of the most consistent security models of authenticating nodes is the use of digital signatures, which are cryptographic computations that provide evidence of legitimacy and vouch authenticity. In a digital signature scheme, the sender computes a message digest using its private key and which is be verified using its public key by the receiver. A successful validation affirms the identity of the sender to the receiver

The most prominent methods for digital signatures in traditional networks are the use of RSA signature schemes [5] with Public Key Infrastructure. They have successfully adopted in commercial applications. However they are computational expensive as they inherently based on large key lengths typically in the range of 1024-2048 bits which is beyond the capability of low computational devices like sensor nodes.

This proposal endeavors to simplify group authentication in sensor groups using the notion of Identity Based Cryptography, specifically using Identity Based Signature Scheme [2]. In this proposal we present a design where the group controller presents a common signing key factoring the group identity as using the above scheme. This allows the group controller to efficiently manage multi node group authentications without the complexity of dealing with multiple public-private key pairs.

2. Related Work

In wireless sensor networks security must be achieved, since it is important to perform various cryptographic operations:

2.1 Authentication in WSN

Authentication is one of the basic measures of ensuring security of networks that helps identify the nodes and devices in the network. Given that sensor network use over the air media for access and communication, it is prudent to deploy authentication methods in any critical sensor network deployment. While authentication can be enforced at any layer in the network stack, access layer authentication is usually the first point of end-node validation. Methods such as TESLA Broadcast Authentication Protocol [9] have focused on leveraging broadcast and multicast message with time synchronization has been proposed that employs symmetric keys.

2.2 Group based Security

Modern network deployments are multi-dimensional with communication requirements beyond one-to-one and unicast. Group and multicast communications are necessary while commanding and controlling set of devices. In such cases group communication is more efficient and a multiple unicast communications. Like unicast communications, group communications also require security and protection against attacks [10].

2.3 Identity Based Cryptography

Identity Based Cryptography though has in existence since the time it was first proposed in early 1980 [1], its application to real world security is just beginning to be explored. Security researchers in areas of sensor network has shown particular interest in the Identity Based Cryptography largely because of the simplified key management scheme which does not require exchange of key material required for security association as well the use of any unique text value identifier such as name of a user or email address or domain name that can be used as public key eliminating the overhead that typically exists with any RSA based cryptography such as Digital Certificates [4]. This makes the use of IBC compelling for use in addressing security needs sensor networks as the nodes can be deployed with textual information as public key. [3] Proposes a scheme of a framework for authentication using Identity Based Signatures in WSN, specifically for authenticating broadcast and multicast messages.

3. Design Methodology

This section describes a high level view of the proposed architecture as presented in Fig. 1

Group Controller - We propose a central authentication approach where all sensors node that from a group authenticate with a Group Controller (GC). The Group Controller is assumed to a resourceful device that can handle considerable number of sensor nodes as group members. It is also tasked with performing cryptographic functions such as System Setup, Key Extraction, Key Refresh, Signature Generation, Signature Verification, Encryption and Decryption,

Group Members –Group Members are sensors nodes that are deemed part of a group. They are required to authenticate with Group Controller for communicating within the group. The Group Member is provisioned with required group specific security credentials before they are deployed into the group.

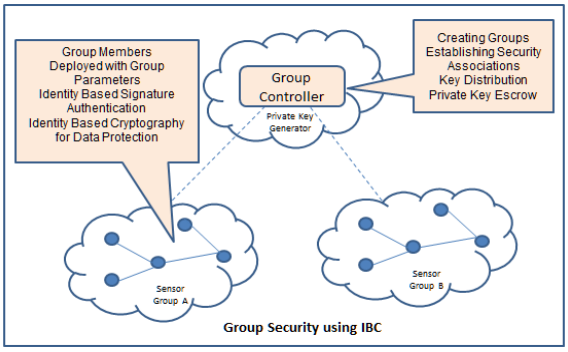

Fig. 1. Group Security using IBC Architecture

3.1 Sensor Group Member Authentication using IBC

There are many deployment scenarios where sensors monitoring and transmit critical information to data acquisition and analytics systems. For example this includes sensors deployed for perimeter security or bio-monitoring sensors that transmit vital metrics, lighting sensors that transmit status to lighting administrators and so on. A data acquisition system should ensure that it receives data from legitimate group nodes and not from any attacker nodes that may feed malicious information or content. The key goal of Sensor Group Member Authentication is to prevent unauthorized access or data transmission within a group. We propose a model based on Identity Based Signature Scheme and is described as follows:

Group Controller Setup – In the approach, the Group Controller is a central authority responsible for group establishment and key management. From a security model point of view it is assumed to be a Trusted and adequately protect from any vulnerabilities. The Group Controller takes a security parameter 1^k which represents a k-bit string of each bit of value 1. i.e., $\{1111111...1_K\}$, and generates a master secret key (MSK) called PvK_{GC} and a group system parameter GP using a Boneh-Lynn-Shacham Short signature scheme based on Weil pairing over elliptic curve and finite fields [7]

$$\{PvK_{GC}, GP\} \leftarrow Setup(\{1111...1111_k\})$$

Group Key Generation – A specific group in the sensor network is identified by a Group Identifier (GID_i) a numeric string of length-n (32-bits). The GID_i is passed to the Group Controller to obtaining a secret key called SK_{GIDi} corresponding to the Group identified by GID_i. The Group Controller uses its master secret key PvK_{GC} to generate private key for the Group.

$$\{ SK_{GIDi} \} \leftarrow \text{Key Generate}(GID_i, PvK_{GC}) \quad (1)$$

Group Member Sensor Node Deployment – When a new sensor node is to be deployed into the network, the new node has to be setup for legitimate participation in group. This is done by obtaining a secret specific to the group to which the sensor node is being made a group member. This process is described as follows:

(i) The member sensor node is assigned a Group Identity (GID_i) to which it intended to become a member.

(ii) The Group ID (GID_i), the private key (SK_{GIDi}) corresponding to the group, the group parameter GP are packed into the member node before being deployed in the sensor network. Members of the same group will have the same security context $\{GID_i, SK_{GIDi}, GP\}$ stored in them.

Group Member Authentication – When a Group Member enters a group it is required to authenticate with the Group Controller by presenting a cryptographic evidence of its authenticity of being member of the claimed group. This process is as follows:

(i) Group Member node create a message p and using any well know hash algorithm creates a signature δ using the group security key (SK_{GIDi}) stored in it.

$$\{ \delta p \} \leftarrow \text{Signature}(p, SK_{GIDi})$$

(ii) Group Member now transmits a message to Group Controller with the message p, corresponding signature δp, its Group Identity GID_i and group parameter GP

$$Tx \leftarrow p \parallel \delta p \parallel GID_i \parallel GP$$

Group Member Validation – When the Group Controller receives an authentication message ($p \parallel \delta p \parallel GID_i \parallel GP$) from a sensor node, it run a validation function that cryptographically verifies the evidence provided. The validation process is as follows:

(i) The Group Controller retrieves the corresponding group secret key (SK_{GIDi}) based on the GID_i provided in the message and computes a signature $\delta p'$ on the message p.

$$\{ \delta p' \} \leftarrow \text{Signature}(p, SK_{GIDi})$$

If the signature computed by Group Controller matches with the signature transmitted by sensor node i.e. $\{ \delta p'$ equals $\delta p \}$ then the sensor node is deemed authenticated and authorized member of the corresponding group.

The proposed system is based on the concept of Identity based signature schemes that provides a simple yet efficient protocol for authentication in sensors. The pre deployment of sensor nodes with group secret key based on the group membership by the administrators helps reduce cryptographic overheads for group member association. Here is a brief security analysis of the protocol scheme.

Threat/ Requirement	Proposed Protocol
Replay Attack	Fulfilled
Cloning Attack	Fulfilled with hardware assist
Man in Middle (MIM) Attack	Not Fulfilled
Chosen Challenge and Response Attack	Fulfilled
Information Freshness	Fulfilled
Confidentiality	Fulfilled
Instant Authentication	Fulfilled
Mutual Authentication	Not Fulfilled
Anonymity	Not Applicable
Integrity	Fulfilled

TABLE I. SECURITY CONSIDERATIONS

4. Experimental Result

In this demonstration there is two scenario where one with group controller authenticating one group member with same signature & another group member with different signature.

Cryptographic algorithm 1: Group Controller

Figure 1.1 shows the cryptographic setup Group Controller Algorithm. In this part the group controller will be assigned with the group controller ID and group system parameter.

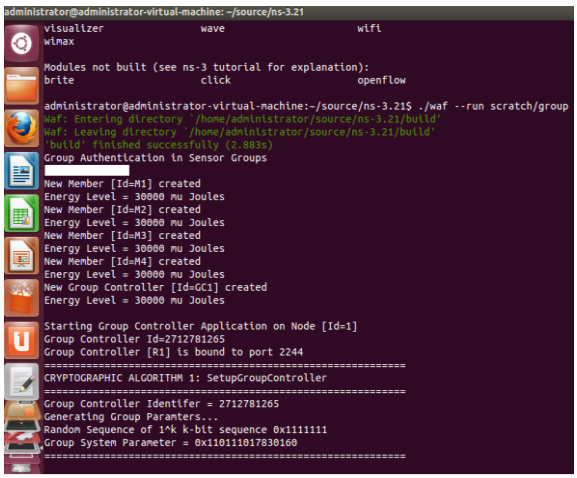

Figure 1.1: Setup Group controller Algorithm

Cryptographic algorithm 2: Group Secret Key Generation

Figure 1.2 demonstrate the cryptographic group secret key generation algorithm where the group controller will generate a secret key called master secret key with the help of Group ID and Group system parameter.

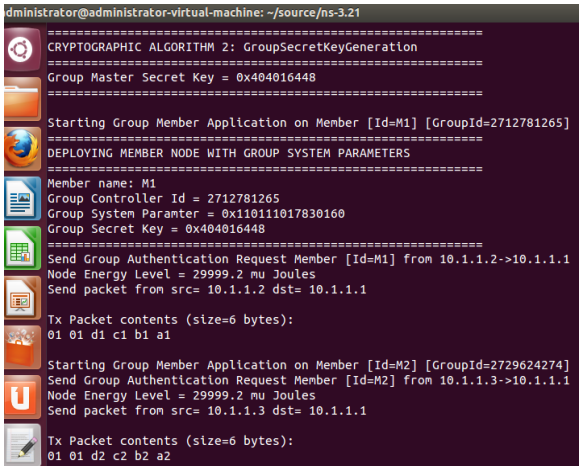

Figure 1.2: Group secret key generation & Group Member Initialization

Cryptographic algorithm 3: Group Message Sign Authentication

Figure 1.3 shows the cryptographic group message sign authentication algorithm. In this simulation the group controller will send the message with timestamp to the group member. The group member will sign the message of controller using hashing with the help of secret key & group ID. This signed message is send to the controller.

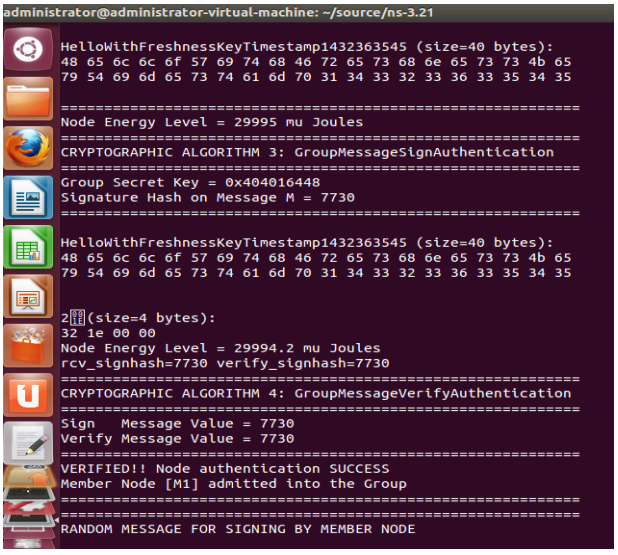

Figure 1.3: Group Message sign authentication

Cryptographic algorithm 3: Group Message Verify Authentication

Figure 1.4 shows the cryptographic group message verify authentication algorithm. In this part the controller will compare the signed message from the member with the message which computes sign in controller. If both the message matches the member will be successfully authenticated.

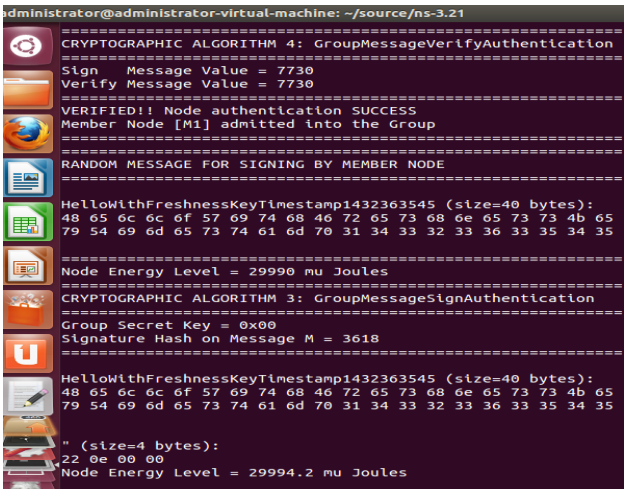

Figure 1.4: Group Message verify authentication

Cryptographic algorithm 4: Group Message Verify Authentication with malicious node

Figure 1.5 shows the cryptographic group message verify authentication algorithm. In this part the controller will compare the signed message from the malicious member node with the message which computes sign in controller. If both the message do not matches the member will be blocked & denied for future accession of data in group.

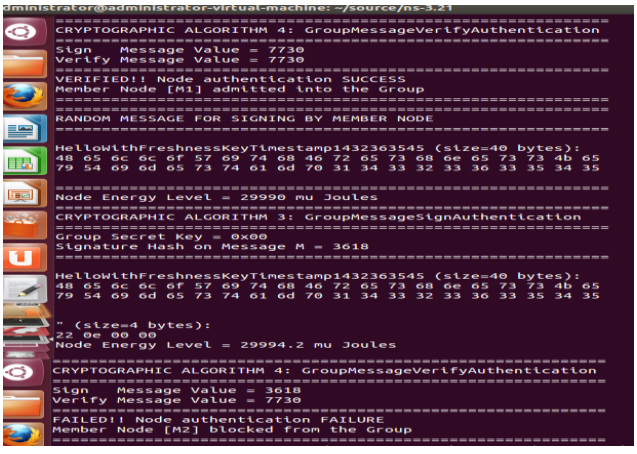

Figure 1.5: Group Message verify authentication for malicious node

5. Conclusion & Future Work

The approach to use Identity Based Cryptography provides a simple yet considerably secure Authentication model in Sensor Groups. The simplicity of the approach of group secret key generation at the time of sensor deployment helps conserve resources on node members.

The next step in the proposed work is to implement the authentication protocol using an Identity Based Signature using a bilinear pairings on sensor node and study the computational and operational efficacy of the architecture.

ACKNOWLEDGEMENT

I would like to thank Dr. Sumithradevi K A, principal, GSSSIETW, Mysuru for her extended support in project and forcing me to put in continuous efforts with properly scheduled deadlines. My contribution and work on this project is a result of help and encouragement from Assistant Prof Smt. Hussana Johar R B, GSSSIETW, Mysuru, who has provided me with the best knowledge about the project. I would like to thank her for invaluable support and guidance.

REFERENCES

[1] Shamir, "Identity-based Cryptosystems and Signature Schemes", Proceedings of Crypto '84, Springer-Verlag, 1984, pp. 47-53

[2] Boneh and Franklin, "Identity-Based Encryptionfrom the Weil Pairing", Proceedings of Crypto '01, Springer-Verlag, 2001, pp. 213—229

[3] Rehana Yasim, Eike Ritter, Guilin Wang, "An Authentication Framework for Wireless Sensor Networks using Identity-Based Signatures"

[4] ITU-T Recommendation X.509 (2005) | ISO/IEC 9594-8:2005, Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks.

[5] Rivest R., Shamir A., and Adleman L., (1978) A method for obtaining digital signatures and public-key cryptosystems, Communications of the ACM, 21 (2): 120-126.

[6] Manali Shah, Shrenik Gala, Narendra Shekokar, "Lightweight authenticaiton protocol used in wireless sensor network", CSCITA,2014

[7] http://jhuisi.github.io/charm/charm/schemes/pksig/pksig_hess.html

[8] Lein Harn and Changlu Lin, "An Efficient Group Authentication for Group Communications", IJNSA, Vol.5,No.3, May, 2013.

[9] Perrig, Canetti, Tygar, and Song, " The TESLA Broadcast Authentication Protocol," In CrytoBytes, Summer/Fall 2002, pp:2-13

[10] Jianmin Zhang , Wenqi Yu and Xiande Liu ,"CRTBA: Chinese Remainder Theorem- Based Broadcast Authentication in Wireless Sensor Networks," in Computer Network and Multimedia Technology, 2009, Wuhan, International Symposiumon 18-20 Jan. 2009

[11] Sandro Rafaeli, David Hutchison, "A survey of Key Management for Secure Group Communication", ACM Computing Surveys,Vol.35,No.3, Sep.2003

[12] John Paul Walters, Zhengqiang Liang, Weisong Shi, and Vipin Chaudhary, "Security in Distributed, Grid, and Pervasive Computing", 2006

BIOGRAPHIES

Asha A, pursuing M.Tech in Digital communication & Networking at GSSSIETW, Mysuru, Her interst are in the fields WSN, Networking, Information coding, Wireless Mobile networks.

Smt. Hussana Johar R B, M.Tech in information & communication system, MCE, Hassan, BE from NIE Mysuru, field of specialization WSN, WBAN, information coding presently she is working as Assistant Professor in the Dept of TE, GSSSIETW, Mysuru.

Dr. B. R Sujatha, PhD degree in AdHoc networks, ME from IISC, field of specialization includes WSN, Wierless AdHoc networks, Mobile Networks, Information coding & cryptography presently she is working as professor in the Dept of ECE, MCE, Hassan.

