ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 5, May 2014

Secure Transmission in MANET and Wireless Sensor Network

Manjunath C R[1], Sindhu Anand[2], Jeevan Yadav N S[3]

Assistant professor, Dept. of CSE, School of Engineering and Technology Jain University , Kanakapura Taluk, Karnataka, India[1]

PG Students [CSE], Dept. of CSE, School of Engineering and Technology Jain University, Kanakapura Taluk, Karnataka, India[2,3]

ABSTRACT: Security is a major issue in any network, having a secure transmission channel for data transmission or a secure communication path from the source to destination is a challenge in MANET and WSN. In MANET, using threshold digital signature is used in existing key management schemes for network. In wireless sensor networks, a security mechanism based on elliptic curve cryptography is considered to provide the authentication for nodes and their identity for message transmission, then certificate is used to check the trustworthiness of the nodes in a cluster for authentication purpose. In this paper summarizes the use the two secure schemes for WSN and MANET.

KEYWORDS: MANET, WSN, Threshold Digital Signature, Elliptic Curve Cryptography, Certificate, Secure Transmission Channel.

I. INTRODUCTION

Security has a major impact on Mobile ad hoc networks (MANETs) and wireless sensor networks (WSNs), Mobile ad hoc networks (MANETs) do not require wired infrastructure or expensive base stations. Nodes within radio range of each other can communicate directly over wireless links, and those that are far apart use other nodes as relays called as intermediate nodes. As Wireless sensor networks usually have more nodes than MANETs, and sensory nodes in WSNs are more resource constrained in terms of power, computational capabilities, and memory, the security design used in WSNs has to be more specific for those areas. Security issues can be categorized and provided through different techniques like key management, and trust in; most of it is associated with authorization, encryption, decryption and authentication are some.

When considering the security aspect, a cryptography technique or scheme can be applied in both MANETs and WSNs in different areas. ID-based cryptography is used to develop a new certificate security scheme in MANETs, which can be used as a one kind of security scheme in vehicular ad hoc networks. MANET and WSN which provides with the latest schemes in cryptographic techniques and bring in new perspective to security, performance, and many other areas of issues for high importance in MANETs and WSNs. The main aim is to find methods in cryptography and its basic applications in MANETs and WSNs builds a foundation for advanced research in security. It aims at providing information/outlook about how MANET and WSN security design can be better achieved with knowledge of cryptography. An approach to form a secure channel establishment using threshold signature scheme for MANET and certificate generation method using public key cryptography for WSN are the technique which have been given importance in proposed work .

II. KEY MANAGEMENT AND KEY DISTRIBUTION

Key [1] [11] management is one of the most important issues of any secure communication. With the increasing demand for the transmission security in wireless sensor networks, the key management can be done in two methods, providing session key to individual nodes and providing key management to group nodes, before exchanging data securely, encryption keys must be established among sensor nodes. Key usage for secure data transmission, it does not specify how to exchange keys securely. Besides the link layer, upper layers such as the network and application layers also must exchange keys securely. This is a challenging problem because there are many stringent requirements for key management, and the resources available to implement such processes are highly constrained. Many security-critical applications depend on key management processes to operate but also demand a high level of fault tolerance. Multiple Keys are distributed among the sensor nodes; each node must broadcast the key's ID within its communication range to find out if the nodes share the same key. A secure communication can be established as long as there is at least one key being shared. If there is no key shared between two nodes, then the link has to be established through two or more paths.

III. SECURE TRANSMISSION IN WSN

A. Key Distribution Schemes:

There are [11] three keying models that are compared between the WSN security and operational requirements which are network keying, pairwise keying, and group keying. The network keying model has advantages over the pairwise keying, and group keying. It is simple, easy to manage, and uses very little resources. It allows collaboration of nodes where neighbouring nodes can read and interpret each other's data, it is self-organizing, scalability and accessible. The drawback of network keying is robustness.

The pairwise keying it is difficult to add new nodes to the network, hence affecting the flexibility requirement. This is a resource-intensive process that uses more energy when compared with the simple preloading of a network-wide key as in the network keying. Some pairwise key distribution are self-organization, because they tackle the scalability problem by reducing the number of shared keys, results in some nodes being unable to communicate with other nodes and hence compromising the self-healing and self-organizing abilities of the network.

The group keying combines the features of both network and pairwise keying techniques. When group of nodes form a cluster, communications are performed using a single, shared key similar to network keying. The communications between group's uses a different key between each pair of groups in a manner identical to the pairwise keying technique. Scalability, increase keys with the number of groups, not with the size of the network. The drawback with this technique is that it is difficult to set up and also the formation of the groups is a very application dependent.

B. Certificate Generation Method:

A WSN consists of hundreds or thousands of densely populated sensor nodes spread over a medium scaled network, which sense the data and propagate through the network. They work collaboratively to process and sensed data. These sensor nodes send data streams to base stations either periodically or based on events and base station send the data to the destination node. In a network, sensors nodes may be densely populated wit, the area detected by the sensors are dividing into a number of small clusters.

A Grid is a cluster based schemes, in which clusters are equally sized square grids in a two dimensional plane, have a simple structure with less routing management overhead. With the assistance of GPS or localization techniques, the square grid also provides easier coordination among all sensor nodes in the network.

The base station plays a major role in forming the secure transmission channel which acts like a gateway for external communication. The base station gathers information of all the nodes from the Grid to form the clusters according to the location of the nodes. A key management mechanism is used which is based on ECC. It provides authentication services for the identity of nodes and message transmission between the source and destination. It provides a mechanism the add nodes with pre-loaded public keys as certificates to help the other nodes verify their trust worthiness. By doing so, the old nodes do not have to update their keys for secure communications with the new nodes.

During the node deployment, each sensor node has to go through an initialization phase, where the base station certifies the trust worthiness of the nodes. The base station generates a pair of public and private keys for each node that issues pre-loaded certificates to ensure the trust worthiness of the newly added nodes. Pre-loaded public key can be used as the certificate to ensure the trust worthiness of the newly added nodes to the network. The nodes within a cluster can verify their trust worthiness with each other within the valid period of certificates generation.

IV. SECURE TRANSMISSION IN MANET

A. Trust Management:

A [13] [12] key aspect for WSN is the trust on the behaviour of the elements of the network. Trust evaluation mechanisms for distributed networks for MANETs and sensor network have been analysed. Where for any trust management system has to be designed and prepared for reacting against the particular issues, such as decentralization and initialization that can be found in WSN environments. The node [15] trust value is calculated based on the cryptographic mechanism being applied, availability statistics and the packet forwarding information about the node. If computed trust value of a node falls below a threshold, the node's location is considered insecure and it is avoided in the routing process.

B. Signature Schemes:

[16] Mobile ad-hoc network security (MANET) is becoming a more entangle problem compared to other networks security. In ad hoc networks the nodes often leaves the network and re-joins frequently. So authentication plays a vital

role when a node joins and re-joins into the network. A digital signature is another part of the security parameter in the network security. A signature is need in the MANET and WSN for detecting the treats and various types of intrusion detection. There are several types of signature scheme used, these schemes helps in identifying the node which are attacked. The signature scheme helps in providing a secure transmission channel for data transmission.

C. Threshold Signature Scheme:

Developed a [17] [12] trust based security protocol based on a cross-layer approach which attains confidentiality and authentication of packets in both routing and link layers of MANETs. Here in the first phase, a design of trust-based packet forwarding mechanism for detecting and isolation of malicious nodes using the routing information are found. Trust values used for each node for packet forwarding by maintaining a trust counter. A node is accepted or rejected by the trust counter while routing process. If the trust counter value falls below a trust threshold, the respected node is marked intermediate as malicious.

To [14] form a secure and effective communication channel a Multi threshold-signature scheme is used which is defined by fundamental properties. A threshold multisignature scheme shows that this scheme satisfies the properties and eliminates the attacks to which other similar schemes are subjected to. Threshold Multisignature schemes combine the threshold signature schemes and group multi signature schemes to yield a signature scheme that allows a threshold or more group members to collaboratively sign an arbitrary message.

In this scheme a novel cluster based secured routing methods that protect packets sent in MANETs from intermediary malicious nodes by attempting to only route them through trusted nodes. The network is organized in such a way that there is one-hop disjoint clusters, for every node elected by the most qualified and trustworthy node of its hop neighbours to be its cluster-head (CH). Cluster members forward packets only through the trusted cluster-heads (CH) thus ensuring a safe communication path. This a different approach for a new threshold-multisignature scheme without a trusted third party, based on a round optimal, publicly verifiable protocol. This scheme can be easily adapted to incorporate a trusted third party; a version of the scheme is where the assistance of a trusted third party will therefore not be presented. A discrete logarithm-based threshold-multisignature scheme is used for secure path. The discrete logarithm-based threshold-multisignature scheme is made secure by periodically updating secret shares and changes the group membership by allowing an authorized subset of existing group members to redistribute secret shares to form a new access structure. This scheme provides an individual signature for each node in the network; a random integer and hash function is used to provide the threshold signature.

V. DISCUSSION

Security has a major impact on Mobile ad hoc networks (MANETs) and wireless sensor networks (WSNs), Key management plays a major role in establishing the communication between the two parties by providing the session key to individual nodes and also key management to group nodes, before exchanging data/nodes securely. Key management processes to operate but also demand a high level of fault tolerance. In Table-1 , provides an overview of different schemes that can considered in secure communication. However the selection of scheme has to be made based on the requirement and level of security needed.

Table1: MANET and WSN schemes and their properties:

SCHEMES	MANET	WSN
Threshold Signature	i. Can be considered in unicast routing. ii. Applicable for Group communication iii. Multilevel security iv. Efficiency is more	i. Restricted, to application specific ii. More energy consumption
ECC+DH	i. Efficient in term of accessibility ii. Less energy consumption iii. No restriction for network topology iv. Smaller key size Applicable	i. Efficient in term of accessibility ii. Less energy consumption iii. Restriction with respect to network topology iv. Smaller key size
Certificate	i. Applicable for node's security	i. Applicable for node's security

The key management schemes ECC, DH and certificate generations holds good for WSN and MANET, but the threshold signature scheme can be used directly in MANET the same is not applicable in WSN due to various constraints.

VI. CONCLUSION

MANET and WSN offer wireless channel communication, establishing the secure transmission channel is challenging task. A threshold digital signature is an important cryptographic tool used in existing key management schemes for mobile ad hoc networks. Where as in a Wireless sensor networks aims at the issues dealing with symmetric key encryption methods. A security mechanism based on elliptic curve cryptography is being used to provide the authentication for nodes and their identity for message transmission. A certificate is used to check the trustworthiness of the nodes in a cluster for authentication purpose. The usage of the secure scheme is depends on the topology and application in small scale network, for large scale network still is challenge.

REFERENCES

[1]. Bin Tian, Yang Xin Shoushan LU0, Xi Ouyang Dong , Li Zhe Gong , Yixian Yang “A Novel Key Management Method For Wireless Sensor Networks” IC-BNMT IEEE 2010.
[2]. T.Thenmozhi, Dr.R.M. Soma Sundaram Dean “Towards An Approach For Improved Security In Wireless Sensor Networks” 26th -28th July 2012 India IEEE 2012.
[3]. Security Yan-Xiao, Xi’an, Qian-Liang “Research On Wireless Sensor Network” International Conference on Computational Intelligence and Security IEEE 2010
[4]. T.Kavitha, S. Jenifa Subha Priya, Dr. D.Sridharan “Design Of Deterministic Key Pre Distribution Using Number Theory”, IEEE 2011.
[5]. Jaydip Sen “Security In Wireless Sensor Networks”, National Institute Of Science & Technology, INDIA
[6]. David Martins And Hervé Guyennet “Wireless Sensor Network Attacks And Security Mechanisms : A Short Survey Computer Science” 13th International Conference on Network-Based Information Systems IEEE 2010.
[7]. Qusay Idrees Sarhana “Security Attacks And Countermeasures For Wireless Sensor Networks: Survey Department Of Computer Science”, International Journal of Current Engineering and Technology, Vol.3, No.2 (June 2013) INPRESSCO 2013.
[8]. S. Jerusha, K.Kulothungan & A. Kannan “Location Aware Cluster Based Routing In Wireless Sensor Networks” International Journal Of Computer & Communication (PRINT): 0975 - 7449, Volume-3, Issue-5, ISSN 2012.
[9]. Ketki Ram Bhakare R. K. Krishna Samiksha Bhakare “An Energy-Efficient Grid Based Clustering Topology For A Wireless Sensor Network” International Journal Of Computer Applications (0975 – 8887) Volume 39– No.14, February 2012.
[10]. D. J. Dechene, A. El Jardali, M. Luccini, And “A. Sauer A Survey Of Clustering Algorithms For Wireless Sensor Networks”.
[11]. Cheng-Lung Yang, Wernhuar Tarng, Kuen-Rong Hsieh And Mingteh Chen “A Security Mechanism For Clustered Wireless Sensor Networks Based On Elliptic Curve Cryptography” IEEE 2010.
[12]. Aravindh S, Vinoth R S And Vijayan R “A Trust Based Approach For Detection And Isolation Of Malicious Nodes In MANET”, IJET Vol 5 No 1 Feb-Mar 2013.
[13]. Mrs. Priti Rathi1, Mr. Parikshit Mahalle “Certificate Revocation In Mobile Ad Hoc Networks” IJAIEM Volume 2, Issue 1, January 2013.
[14]. D.S.Dawoud, P.Dawoud, J.Van Der Merwe, C.Ndagije “A New Threshold Multisignature Scheme For Mobile Adhoc Networks” Second International Conference on Advances in Engineering and Technology ICAET 2011.
[15]. Marco Fiore, Claudio Casetti, Carla-Fabiana Chiasserini, Panagiotis Papadimitratos “Discovery and Verification of Neighbor Positions in Mobile Ad Hoc Networks” version 1 - 15 Oct 2013 IEEE 2013.
[16]. Sattar J Aboud Mohammad AL-Fayoumi “Efficient Threshold Signature Scheme”, Vol. 3, No. 1, IJACSA 2012.
[17]. Philip England, Dr Qi Shi, Dr Bob Askwith, Dr Faycal Bouhafs “A Survey of Trust Management in Mobile Ad-Hoc Networks” ISBN: 978-1-902560-26-7 2012 PGNet.
[18]. Parvinder Singh, Dinesh Singh and Vikram Singh “Evaluation of Routing Protocols in MANETs with Varying Network Scope” IPCSIT vol. 37 ICINT 2012.
[19]. Daxing Wang, Jikai Teng “Id-Based Aggregate Signature Scheme and Its Application in Authenticated Routing”, Vol.12, No.1, January 2014, pp. 802 ~ 808 Indonesian Journal of Electrical Engineering 2013.
[20]. Hu Xiong, Zhiguang Qin, and Fagen Li “Identity-based Threshold Signature Secure in the Standard Model” International Journal of Network Security Vol.10, No.1, PP.7{80, Jan. 2010.
[21]. Sharad Kumar Verma1, Dr. D.B. Ojha “New System Security Model for a Mobile Operator’s Meshed Access Network” IJIRCCE Vol. 1, Issue 6, August 2013.