ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Security in Wireless Sensor Networks Using Crypto Techniques

R.Uday Kumar
M.Tech Student,
Dept of CSE,
PCET, Nellore, India.

G.Yedukondalu
Asst Professor,
Dept of CSE,
PCET, Nellore, India.

D.Venkatasubbaiah
Associate Professor,
Dept of CSE,
PCET, Nellore, India.

Abstract:

In hop by hop message authentication with source privacy in wireless sensor network, were authentication is effective way to protect from unauthorized users effected messages from being send through in wireless sensor networks. confidentiality and security to the data is actually provided by an authentication . Authentication involves the confident identification of one party by another party or a process of confirming an identity.

Many message authentication schemes have been used to protect messages but these authentication schemes have the limitations of high overhead, lack of ability, to node attacks and threshold problem. Message authentication has a main role in thwarting unauthorized and effected messages from being sent in networks to save the energy.

Many authentication processes have been implemented to provide message authenticity and verification for wireless sensor networks. There were various methods have been developed to solve the problem such as symmetric key cryptography and public key cryptography. Each would have their own problems such as threshold overhead and key management and computation overhead and scalability.

In order to solve such problem we developed a new authentication scheme using the elliptic curve cryptography. In this scheme any node can transmit n number of message without threshold problem. This paper is to do survey before actually implementing it.

Keywords :

Authentication schemes, multicast networks, key management, symmetric key, public key.

I.INTRODUCTION :

The System which allows the sender to send a message to the receiver end insuch a way that if the modified message will almost detected by Receiver that termed as message authentication. We can also say that message authentication is data origin authenticity. Protecting the integrity of a message is done by message authentication. Each user while using message authentication expects that each and every message should be pass as in same condition that it was sent without adding any modified bits or extra characters. Wireless sensor have special characteristics because of total absence of infrastructure or administrative support these are wireless networks.

They have limited bandwidth, energy constraints, low computational capabilities. Instead of all limitation WSN in useful in where is communication is done without infrastructure support. Security is the major constraint in WSN ,as sensor node may be deployed by attacker and the private information may get hacked . In many cases it is sufficientto secure data transfer between the sensor nodes and the base station. In particular, the base station must be able to ensure that the received message was sent by specific sensor node and not modified while transferring. Many WSN applications such as health-care monitoring systems or military domains needs strong and lightweight authentication schemes to secure data from unprivileged users. That is really insecure.

To over come all such security issue many different scheme that had been discover. Some schemes deals with detecting the compromised node , or detecting the injected false message in the network or giving special authorization to the sender or receiver, Encryption of decryption is the famous method for providing the security.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

II.MESSAGEAUTHENTICATIONS TECHNIQUES:

Statistical mechanism that can detect and drop such false reports. It requires that each sensing report be validated by multiple keyed message authentication codes, each message generated by a node that detects the same event. If the report is forwarded, all nodes along the way verifies the correctness of the MACs probabilistically and drops those invalid MACs at earliest points. The sink further filters out remaining false reports that escape the en-route filtering. It exploits the network scale to determine the truthfulness of each report through collective decision-making by multiple detecting nodes and collective false-report-detection by multiple forwarding nodes. Our analysis and simulations show that, with an overhead of 14 bytes per report, It is able to drop d false reports by a compromised node within limited forwarding hops, and reduce energy consumption in many cases.

There is Public key cryptography scheme is used in existing system and proposed system is working on the three different techniques. these are, Public key cryptography based, Symmetric keys and hash functions and one way key chain based on hash functions. In WSNs, it is usually assumed that public key cryptography can not be used because of the elaborate constraints. This means that the two communicating entities must use secret key functions and hash functions. In WSNs, there are two types of authentication: device level authentication and group level authentication. The device level authentication means that a message is proved to originate from a certain device, whereas the group level authentication means a message is proved to originate from a certain group of devices.

III.LITERATURE SURVEY:

Efficient Authentication over lossy channel[1] paper introduced efficient schemes, TESLA and EMSS, for secure lossy multicast streams. TESLA, short for Timed Efficient Stream Loss-tolerant Authentication, offers sender authentication, strong loss robustness, high scalability, and minimal overhead, at the cost of loose initial time synchronization and slightly delayed authentication. EMSS, short for Efficient Multi-chained Stream Signature,provides no repudiation of origin, high loss resistance, and low overhead, at the cost of slightly delayed verification.

Attacking cryptographic scheme[2] show attacks on several cryptographic that haverecently been proposed for achieving various security goals in sensor networks. They also told that these schemes all use "perturbation polynomials" to add "noise" to polynomial-based systems that offer information theoretic security, in an attempt to increase the resilience threshold while maintaining efficiency. They show that the heuristic security arguments given for these modified schemes do not hold, and that they can be completely broken once we allow even a slight extension of the parameters beyond those achieved by the underlying information-theoretic schemes .R.L. Rivest, A. Shamir, and L. Adleman[3] proposed a Method for Obtaining Digital Signatures and Public-Key Cryptosystems. They also show that a message is encrypted by representing it as a number M, raising M to a publicly specified power e, and then taking the remainder when the result is divided by the publicly specified product, n, of two large secret prime numbers p and q. Decryption is similar.

The security of the system rests in part on the difficulty of factoring the published divisor, n Comparing Symmetric-Key and Public-Key Based Security Schemes[4] proposed a system thatbuilds the user access control on commercial off-the-shelf sensor devices as a case study to show that the public-key scheme can be more advantageous in terms of the memory usage, message complexity, and security resilience. They also does work to provides insights in integrating and designing public-key based security protocols for sensor networks. The signature scheme introduced by author David Pointcheval and Jacques Stern[5] .In this paper, they address the question of providing security proofs for signature schemes in the so-called random oracle model . They establish the generality of this technique against adaptively chosen message attacks. Our main application achieves such a security proof for a slight variant of the El Gamal signature scheme where committed values are hashed together with the message.

IV.PROPOSED SYSTEM:

The proposed system is basically design to authenticate the message in network while transferring. There are variety if schemes were discus that follows the authentication method in order to provide the security. The following are the key features of the proposed system that give me the desire effect.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

1)Unconditional source anonymity can be provided by developing the original message authentication code on elliptic curve.

2) Efficient hop by hop message authentication can be achieve without the any limitation.

3) The scheme is prevented by node compromise attacks. The nodes can be secure even if the other node gets compromised.

4) Efficient Key managements were introduced.

V. RESEARCH METHODOLOGY:

The proposed authentication scheme aims at achieving the following goals, Message authentication: The receiver should be able to verify whether a received message is sent by the node or not Message integrity: The receiver should be able to verify whether the message has been modified en-route by the adversaries. Hop-by-hop message authentication: Every forwarder on the routing path or network should be able to verify the authenticity and integrity of the messages upon each reception.

Identity and location privacy: The adversaries cannot determine the message senders ID and location by analyzing the message contents or by the local traffic. Node compromise resilience: The scheme should be resilient to node compromise attacks. No matter how many nodes are compromised an d the remaining nodes can still be secure.

System Model:

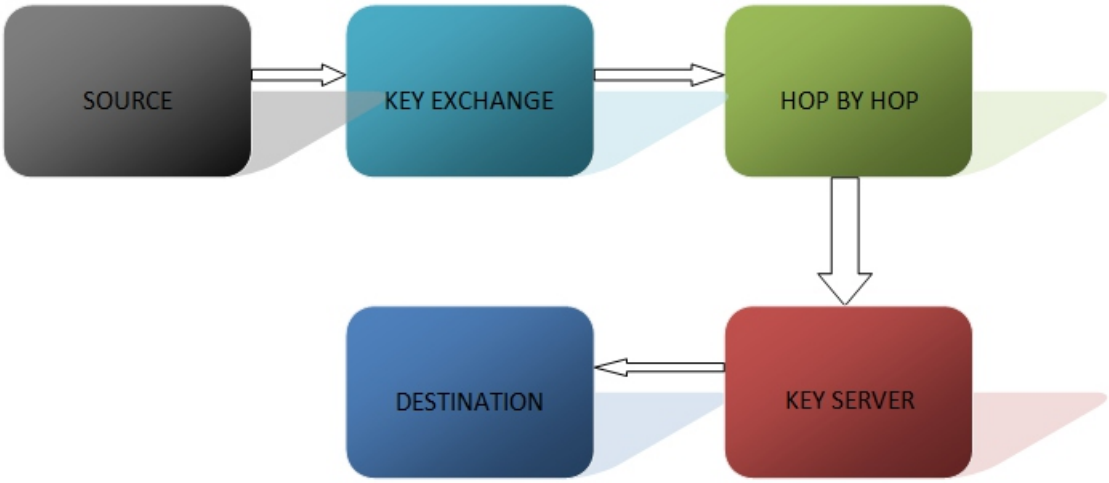

Fig1 :System model

VI.IMPLEMENTATION CONSTRAINTS

Path Selection:

We would like to develop a distance-vector based mechanism. In the traditional distance-vector mechanism, a node only has to advertise the information of its own best path to its neighbors. Each neighbor can then identify its own best path. If a node only advertises the widest path from its own perspective, its neighbors may not be able to find the widest path. In order to assure that the widest path from each node to a destination can be identified, a trivial way is to advertise all the possible paths to a destination. This is definitely too expensive. On the other hand, as long as we advertise every path which is a subpath of a widest path (e.g., <v; a; b; c; d> is a subpath of the widest path of <s; v; a; b; c; d>), we allow every node to identify its own widest path. Thus, to reduce the overhead, we should not advertise those paths that would not be a subpath of any widest path.

Isotonic Path Weight :

We introduce our new isotonic path weight, while the next section describes how we use the path weight to construct routing tables.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

The isotonicity property of a path weight is the necessary and sufficient condition for developing a routing protocol satisfying the optimality and consistency requirements. Given two paths p1 and p2 from a node s to d, assume that p1 is better than p2 by comparing their weights. If the path weight used is left-isotonic, given any path p0 from a node v to s, p0 p1 must be better than p0 p2. Available bandwidth of a path alone is not leftisotonic.

Table Construction and Optimality :

The isotonicity property of the proposed path weight allows us to develop a routing protocol that can identify the maximum bandwidth path from each node to each destination. In particular, it tells us whether a path is worthwhile to be advertised, meaning whether a path is a potential subpath of a widest path. In our routing protocol, if a node finds a new nondominated path, it will advertise this path information to its neighbors. We call the packet carrying the path information the route packet. Based on the information contained in a route packet, each node knows the information about the first four hops of a path identified. Each node keeps two tables: distance table and routing table. Node s puts all the nondominated paths advertised by its neighbors in its distance table. It keeps all the nondominated paths found by s itself in its routing table.

Packet Forwarding and Consistency :

In a traditional hop-by-hop routing protocol, a packet carries the destination of the packet, and when a node receives a packet, it looks up the next hop by the destination only. In our mechanism, apart from the destination, a packet also carries a Routing Field which specifies the next four hops the packet should traverse. When a node receives this packet, it identifies the path based on the information in the Routing Field. It updates the Routing Field and sends it to the next hop. In our packet forwarding mechanism, each intermediate node determines the fourth next hop but not the next hop as in the traditional mechanism. Our packet forwarding mechanism still requires each intermediate node to make route decision based on its routing table. Besides, only the information of the first few hops of a path is kept in the routing table in each node and the routing field in a packet.

Therefore, our mechanism possesses the same characteristics of a hop-by-hop packet routing mechanism, and is a distributed packet forwarding scheme.

Route Update:

After the network accepts a new flow or releases an existing connection, the local available bandwidth of each node will change, and thus the widest path from a source to a destination may be different. When the change of the local available bandwidth of a node is larger than a threshold (say 10 percent), the node will advertise the new information to its neighbors. After receiving the new bandwidth information, the available bandwidth of a path to a destination may be changed. Although the node is static, the network state information changes very often.

Therefore, our routing protocol applies the route update mechanism in DSDV . Based on DSDV, each routing entry is tagged with a sequence number which is originated by the destination, so that nodes can quickly distinguish stale routes from the new ones. Each node periodically transmits updates and transmits updates immediately when significant new route information is available. Given two route entries from a source to a destination, the source always selects the one the larger sequence number, which is newer, to be kept in the routing table. Only if two entries have the same sequence number, our path comparison is used to determine which path should be kept.

Due to the delay of the route update propagation, it is possible that route information kept in some nodes is inconsistent. For instance, the widest path kept in the routing table may not be the widest anymore. Routing loops may occur as well. The situations are referred as inconsistency due to transient route updates, which is different from the definition used in. In and this paper, we consider whether packets can be routed on the computed widest path when the routing tables are stable.

How to avoid loops when routing tables change is an important but difficult problem, and is outside the scope of this paper. We refer readers to [29] for the techniques to reduce route update inconsistencies in the distance-vector protocol which can be applied in our mechanism as well.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

VII.CONCLUSION:

In order to secure your communication message authentication in very important. Through proper message authentication only one can achieve great security. Security is the only seed that plant the proper tree of authenticity. This paper is a survey paper in order to investigate the different techniques available in message authentication. As per the further proceeding my plan is to develop the a new efficient authentication scheme using the elliptic curve cryptography. In this scheme any node can transmit n number of message without threshold problem. This service is usually provided through the deployment of a secure message authentication code(MAC).

VIII. REFERENCE:

[1] M. Albrecht, C. Gentry, S. Halevi, and J. Katz, "Attacking Cryptographic Schemes Based on 'Perturbation Polynomials'," Report 2009/098, http://eprint.iacr.org/, 2009.

[2] "Cryptographic Key Length Recommendation," http://www.keylength.com/en/3/, 2013.

[3] W. Zhang, N. Subramanian, and G. Wang, "Lightweight and Compromise-Resilient Message Authentication in Sensor Networks," Proc. IEEE INFOCOM, Apr. 2008.

[4] H. Wang, S. Sheng, C. Tan, and Q. Li, "Comparing Symmetric-Key and Public-Key Based Security Schemes in Sensor Networks: A Case Study of User Access Control," Proc. IEEE 28th Int'l Conf. Distributed Computing Systems (ICDCS), pp. 11-18, 2008.

[5] Q. Liu, Y. Ge, Z. Li, H. Xiong, and E. Chen, "Personalized Travel Package Recommendation," Proc. IEEE 11th Int'l Conf. Data Mining (ICDM '11), pp. 407-416, 2011.

[6] Q. Liu, E. Chen, H. Xiong, C. Ding, and J. Chen, "Enhancing Collaborative Filtering by User Interests Expansion via Personalized Ranking," IEEE Trans. Systems, Man, and Cybernetics, Part B: Cybernetics, vol. 42, no. 1, pp. 218-233, Feb. 2012.