International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2014): 5.611

Secure Anonymity Communication Protocol for Wireless Sensor Network

Karan Mashal[1], Kajal Mungase[2]

[1]HOD, Computer Engineering Department, RMD Sinhgad School of Engineering, Savitribai Phule University, Pune, India

[2]ME student, Computer Engineering Department, RMD Sinhgad School of Engineering, Savitribai Phule University, Pune, India

Abstract: ***In wireless sensor networks becoming more and more important for sensor nodes to maintain anonymity while communicating data because of security reasons. Anonymous communication among sensor nodes is important, because sensor nodes want to cover up their identities either being a base station or source node Existing anonymity schemes for wireless sensor networks either cannot realize the complete anonymities, or they are suffer from various overheads such as huge memory usage, complex computation. The existing system presenting an efficient secure anonymity communication protocol (SACP) for wireless sensor networks that can realize complete anonymities offering overheads with respect to storage, computation and communication costs. The proposed system accomplishes the task of source, destination and intermediate node anonymity using the proposed algorithm. Our approach source encrypts the packet using destinations public and employ a changing virtual destination to main the source and destination anonymity.***

Keywords: Encryption, Decryption, Security, Wireless sensor network, RSA Algorithm, Hashing, Virtual Node

1. Introduction

Anonymity of sensor nodes in wireless sensor networks can avoid attacker from identifying the message originator node and also evades from capturing important nodes such as source node and base station nodes. Generally, the sensor nodes are arranged in hostile environment, for example in war zones, boarders, battlefields, so securing the communication among these sensor nodes is important. Numerous researchers are working intensively on security issues in wireless sensor networks. However, anonymity is very significant in maintaining the node un traceability, unlink ability, and location privacy of node, but anonymity is not studied and implemented very thoroughly.

In this paper we present a secure anonymity communication protocol (SACP) for wireless sensor networks. This protocol avoid an attacker from discovering the location of the source sensor node and the destination sensor node. In this paper, the presented scheme offers three types of anonymities: sender node anonymity, base station anonymity, and data communication association anonymity and the given scheme is using symmetric cryptography and hash function requiring little computation.

2. Literature Review

2.1 Efficient anonymity schemes for clustered wireless sensor network

Authors: Satyajayant Misra and Guoliang Xue

In this paper, they proposed two simple and efficient schemes for establishing anonymity in Clustered Wireless Sensor Networks (CWSNs). The schemes apply to a CWSN in which the nodes in a neighborhood share pair wise keys for authentic and confidential communication. The first scheme, named Simple Anonymity Scheme (SAS), uses a range of pseudonyms as identifiers for a node in the network to ensure concealment of its true identifier (ID). After deployment, neighboring nodes in the network share their individual pseudonyms and use them to ensure that the communication is anonymous, and a node's true ID is kept private. The second scheme, named Cryptographic Anonymity Scheme (CAS), uses a keyed cryptographic one way hash function to ensure ID concealment. In this scheme, after deployment, nodes in a neighborhood securely share the information that is used by a hash function to generate pseudonyms that are used by the communicating nodes instead of their true ID.

2.2 Anonymous Path Routing in Wireless Sensor Networks

Authors: jehn-ruey jiang , jang-ping sheu , ching tu

In this paper general solutions of secure data communication are to encrypt the packet pay load with symmetric keys. But those solutions only prevent the packet content from being snooped or tampered. Adversaries still can learn of network topology by the traffic analysis attack for starting devastating attacks such as the denial-of-service attack and the like. In this paper, they propose an anonymous path routing (APR) protocol for WSNs. In APR, data are encrypted by pair-wise keys and transmitted with anonyms between neighboring sensor nodes and anonyms between the source and destination nodes of a multi-hop communication path. The encryption prevents adversaries from disclosing the data, and the anonymous communication prevents adversaries from observing the relation of the packets for further attacks.

2.3 Location privacy and anonymity preserving routing for wireless sensor networks.

Authors: Alireza A. Nezhad

In this paper, they explain that appropriate solutions for problem depend on the nature of the traffic generated in the network as well as the capabilities of the adversary that must be resisted. When there is a sufficient amount of data flows

(real or fake packets). They proposed Destination Controlled Anonymous Routing Protocol for Sensor networks DCARPS anonymous routing protocol can support location privacy against a global eavesdropper. Otherwise, it is only possible to stop packet tracing attacks by a local eavesdropper, which is what our probabilistic DCARPS protocol achieves. These protocols are based on label switching, which has not been used in this kind of network before. To enable DCARPS, they propose a new approach for network topology discovery that allows the sink to obtain a global view of the topology without revealing its own location, as opposed to what is common today in sensor networks. In order to resist traffic analysis attacks aiming at locating nodes, we have used layered cryptography to make a packet look randomly different on consecutive links. A stochastic security analysis of this protocol is provided. Another important issue in resource-constrained sensor networks is energy conservation. this protocol use only modest symmetric cryptography. Also, the sink is responsible for all routing calculations while the sensors only perform simple label swapping actions when forwarding packets. Another advantage of labels is preventing unnecessary cryptographic operations as will be seen in the manuscript. Furthermore , embedded a fairness scheme in the creation of the routing tree for the sensor network that distributes the burden of packet forwarding evenly.

2.4 AICN: An Efficient Algorithm to Identify Compromised Nodes in Wireless Sensor Network

Authors: Rongxing Lu

In this paper how to identify these compromised nodes in a wireless sensor network is a very important security issue. To solve this problem, they propose an efficient algorithm, called AICN, to logically identify the compromised nodes in an capable and useful way. Wireless sensor networking is an emerging technology, which potentially supports many emerging applications for both civilian and military purposes, ranging from environmental monitoring to battlefield surveillance. However, since sensor nodes are inexpensive devices, which could be easily compromised and controlled by an adversary, the compromised nodes could report false sensed results and degrade the reliability of the whole network.. Based on the network reliability estimation (NRE), we also present its enhanced version to further improve the efficiency.

3. Proposed System

The network route from sender node to a destination node may require number of intermediate nodes to forward packets for create a multi hop path from a sender to destination. The role of the routing protocol in an ad hoc network is to allow nodes to learn such multi hop paths[1].

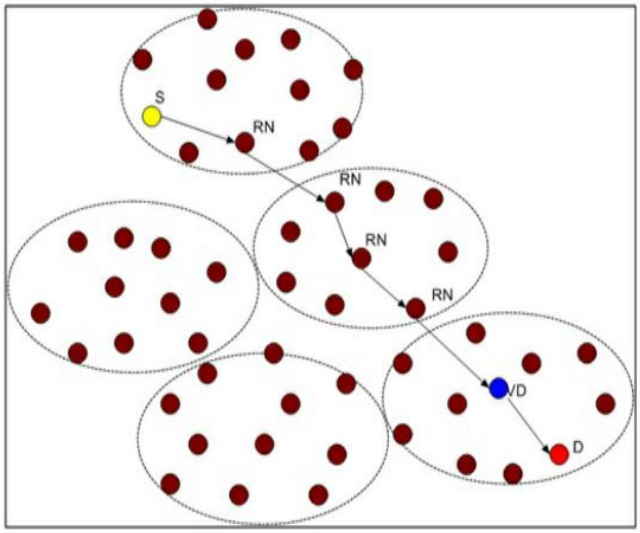

Figure 1: System architecture

3.1 Create network and Locate Source and destination:

In this module initially, the network is created using the specified number of nodes. Source and destination nodes are located in the network. In order to perform a routing next task is to create the zones in the network.

3.2 Create Zones

In this module after locating source and destination nodes in the network, zones are created in the complete network. Zones are created by clustering the nodes in the network. Each node in the zone can communicate the nodes in that zone if it is in its range; otherwise the intermediate nodes are used to forward the packet. Nodes in the one region can communicate with the nodes in the other region nodes which are in the coverage. To maintain the anonymity of the nodes in the network, we route the packet to the virtual destination (VD) in the target zone. This virtual destination in a target zone helps to maintain the destination anonymity. The virtual destination in the network are changed during the each new topology in order to keep the source and intermediate nodes anonymity

3.3 Perform Routing

Routing from source to destination is accomplished by the following steps. Each node in the network creates the secret key (Ks) and public key (Kp) for all nodes in the network. Once the source and destinations are identified, source node generates packet for the destination node and encrypts the packet using public key (Kp) of the destination. Destination on the other hand decrypts the packet using its private key. Source node adds the virtual destination as destination of the packet and forward packet to the virtual destination in the target zone. The virtual destination is elected in each target zone where the actual destination is present. The virtual destination is changed after every topology change in the network to maintain the destination node anonymity.

Once the packet is received by the virtual destination the packet is broadcasted to the few selected nodes in that zone.

As packet is encrypted using the public key of the destination, therefore the packet can be decrypted using the private key of the destination.

4. Conclusion and Future Scope

From this paper we concluded there is routing scheme maintains the source, destination and intermediate node anonymity. Source node encrypts the packet using the destination public key send the packet to the destination, this maintain the destination node anonymity. The virtual destination in the network are changed during the each new topology in order to keep the source and intermediate nodes anonymity. As each time the virtual destination is changed the nodes over the path will automatically changed. Anonymous communication among sensor nodes is important, because sensor nodes want to hide their identities either being a base station or being a source node Existing anonymity schemes for wireless sensor networks either cannot realize the complete anonymities, or they are suffer from various overheads such as enormous memory usage, complex computation. This capability to change the virtual destination in the target zone allows us to keep the anonymity of the source node, intermediate node and the destination node. We used symmetric cryptography and hash function requiring little computation.

References

[1] Kanwalinderjit Kaur Gagneja, " Secure Communication Scheme for Wireless Sensor Networks to maintain Anonymity", International Workshop on Sensor, Peer-to-peer and SociAl Networks, ICNC Workshop 2015.
[2] Alireza A. Nezhad, "Location privacy and anonymity preserving routing for wireless sensor networks ", Journal of Computer Networks, vol.52, no.18, pp.3433-3452, 2008.
[3] Lazos L. and Poovendran R., "SeRLoc:Secure range-independent localization for wireless sensor networks," in Proc. of ACM Workshop Wireless Security, 2004.
[4] Kao J.C., and Marculescu R., "Real-time anonymous routing for mobile ad hoc networks," in Proc. of IEEE Wireless Communications and Networking Conference (WCNC'07), 2007
[5] Satyajayant Misra and Guoliang Xue, "Efficient anonymity schemes for clustered wireless sensor networks" in IEEE ACM Transactions on Networking, Vol. 15, No. 2, pp.55-76, April 2007.

Author Profile

Prof. Karan Mashal is the Professor of Computer Dept. at RMD SSOE, Pune, having more than 5+ years of experience in the field of teaching and research. The domains of his research are Software Testing, Software Engineering and Web Security.

Mrs. Kajal Mungase-Vatekar is pursuing her Masters of Engineering in the Computer Engineering Department, Sinhgad School of Engineering, Savitribai Phule University Pune. She received Bachelor of Engineering degree in Information Technology from University of Pune, Maharashtra, India.