ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 7, July 2015

Proximity Based Security Technique for Mobile User in Wireless Networks Using Multilevel Session Aggregation

Chetna D. Salame, Prof. Shripadrao Biradar

M.E, Department of Computer Engineering, R. M. D. Sinhgad College of Engineering, Pune, India

Professor, Department of Computer Engineering, R. M. D. Sinhgad College of Engineering, Pune, India

ABSTRACT: Establishment of secure communication between wireless devices/nodes that do not share a prior trust relationship is an important problem. Today's location-sensitive service relies on users mobile device for determining its location and send it to the application. Data aggregation is a key challenging task in wireless senor network to minimize energy consumption and guarantees the data security and reliability. Multi-level data aggregation technique assures security and reliability of data aggregation in the presence of secure routing. We propose a privacy-preserving proximity-based multilevel reliable data aggregation security system for location-based services in wireless networks, without requiring any public key infrastructure, trusted authority or early required secret. In this system, the proximity based authentication and multi level session key establishment are implemented based on temporal location tags. Combining the unique physical features of the signals which may be sent from more than one ambient radio sources, the location tags cannot be easily faked by attackers. More specifically, Distributed data server (DDS) which is the uppermost level builds a public location tag according to some parameters of ambient packet i.e. sequence numbers, received signal strength indicators, and media access control (MAC) addresses. DDS also keeps a secret location tag contain the packet arrival time information which will helpful in generating multilevel session key. As DDS never expose their secret location tags, this system is vigorous against spoofers and eavesdroppers outside the proximity range. Moreover, by exploiting the packet arrival time of the ambient signals the multi level session key establishment strategy will significantly increases the key generation rate.

KEYWORDS: Authentication, Encryption, Wireless sensor network, Multi-level data aggregation, Distributed data server, Session ID.

I. INTRODUCTION

The Wireless Sensor network is distributed event based systems that differ from conventional communication network. Sensor network has severe energy constraints and redundant low data rate. Aggregation is a technique to avoid redundant information to save energy and other resources. The permeation of smartphones and social networks development has grown rapidly in location-based services (LBS), such as the request of the location-based mobile advertising and the nearest business. Secure and reliable location-based services request for secure and accurate proximity tests, which permit radio users and/or service providers to investigate whether a sensing node is located within the same geographic area. Proximity tests have to make available location privacy protection and location unforgeability in order to support the business or financial oriented LBS services.

In Wireless sensor networks (WSNs), multiple small sensors are gathering the sensed data and rely on multihop small range radio communication to send data to the sink node. WSNs can operate in regular continuous monitoring model or an event driven model for data collection. In this paper, a regular continuous monitoring model is selected, where each sensor will manage its area and sends the collected sensed data periodically to the base station possibly through the relay of other sensors or storage nodes, where the storage nodes are something special than the ordinary sensors due to additional computation such as data aggregation and shield the data for secure communication and its having more storage capacity. The key objective of data aggregation is to collect and combine data in an energy efficient way so that lifetime of network is incresed, however, it depends on beneficial energy saving strategies such as

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 7, July 2015

information processing and sensor scheduling to minimize the network utilization. One of the important network processing is data aggregation. The sensors are usually loosely distributed in a sensor field and each of these sensor nodes has the abilities to gather data and send back to the base station through multilevel infrastructure architecture. Energy conservation is the vital factor in sensor network because some amount of energy is used up during data transmission. Data aggregation is the noble technique to save the useful energy of sensor nodes. In most of the wireless sensor networks, the sensors percept the environment based on its desired application and send back to the base station to combine all the information to generate the desired output for user needs. Here, the number of packets are minimized to transmit in the network and can save the energy of sensor nodes because of data aggregation where packets are combined before reaching the base station. Data confidentiality is achieved before encrypting data at source node and decrypting it at destination node for processing. However, any encryption techniques may be required by data aggregation for data communication during aggregation. In WSN, data aggregation is achieved to eliminate reduce data transmission , data redundancy and improve data accuracy.

This paper suggests a robust and secure way to establish communication between mobile users using location tags in multilevel. There are three levels in the network which are Level 1, Level 2 and Level 3. Level 3 is the upper most level which is having information and data about all the lower levels. In lower levels, other nodes i.e. base station, storage node and sensing nodes are present in the form of hierarchy. Here as our contribution we will use multilevel location based session aggregator. So it makes system more secure.

In proposed work using multilevel session key establishment algorithm keys will be generated for each level. The details of this technique will be discussed in further sections.

II. RELATED WORK

In the literature survey section we are going to discuss about recent methods on WSN security approaches:

Liang Xiao, Qiben Yan, Wenjing Lou, Guiquan Chen, and Y. Thomas Hou [2] this paper first introduce Amigo, an algorithm that extends the Diffie-Hellman key exchange with verification of device co-location. They showed that by using knowledge of dynamic characteristics of device's common radio environment as proof of physical proximity, it is possible to securely pair devices that come within close proximity. Because signatures are only used to authorize exchanged key, but not for encryption, after authentication takes place, signature do not remain secret.

Zhu and Guohong Cao, [3] in this paper, a privacy-preserving location proof updating system, called APPLAUS was proposed, which explains co-located Bluetooth enabled mobile devices mutually create location proofs, and transfer to the location proof server. To protect source location privacy from one another, and from the distrusted location proof server, they use statistically changed pseudonyms for each device. Further, they also develop user-centric location privacy model in which individual users evaluate their location privacy levels in real-time and decide whether and when to accept a location proof exchange request based on their location privacy levels. Larger key size have better security level but needs more computation and storage resource.

A. Kalamandeen, A. Scannell, E. de Lara, A. Sheth, and A. LaMarca [4], in this paper Ensemble is introduced which is a system that determines if two devices are in close physical proximity by taking advantage of the similarity of the channel between these devices and a third, observing device. This system leverages the many devices that users already possess to aid in this process. This system is not environment specific, does not require any recalibration, works for different hardware and is robust against several types of attacks, including impostor and man-in-the-middle attacks. But, Esemble is able to decide attackers situated atleast 2m away.

Narendran Thiagarajan , Arvind Narayanan, Mugdha Lakhani, Michael Hamburg, Dan Boneh [5], in this paper, authors presented a variety of cryptographic protocols motivated by and optimized for practical constraints. While they have built a prototype implementation, it remains to be seen if any vendors of location-based services will deploy cryptographic systems in the market. But, in some situation user may not be comfortable for broadcasting.

Nilothpal Talukder and Sheikh Iqbal Ahamed [6], in this paper authors described a serious privacy problem of LBS called multi-query attack. In this attack, the detects location of the service requester can be inferred by the

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 7, July 2015

adversary through obtaining cloaking regions that are shrunk or conclude in occuring queries. This problem can be addressed by non injudiciously retaining, over a duration of time, the cloaking regions for the same set of users. ANNC (Adaptive Nearest Neighborhood Cloaking), prominences expanding disjoint sets of users dynamically over time in order to share the common CRs. The CRs are arrangeed in balanced binary trees with restricted height. Thus ANNC gains the balance between quality of cloaking and search efficiency with higher anonymity levels. The issue with system is that density control of the point-of-interest is temporary at provider's end and supplementary overhead of filtering the result set is now task of query issuer.

Suhas Mathur, Rob Miller, Wade Trappe, Alexander Varshavsky, and Narayan Mandayam [7], in this paper author shows how by using their correlated channel measurements from ambient wireless signals to form a shared crypto-key, wireless devices in proximity can pair autonomously. The speed with which users can securely pair depends on their physical separation, and on the rate of temporal variation in the chosen channels. By monitoring multiple sources simultaneously, or by manually shaking the legitimate devices together, pairing can be accelerated. Using changes in phase, in place of amplitude variations proves to be secure against active attacks. Finally, ProxiMate can be enhanced to allow establishing a common secure association for more than two devices.

III. PROBLEM STATEMENT

In wireless sensor networks, mobile users are vulnerable to different types of attack, especially in a location based services (LBS). To deal with such attacks, and make network more secure and robust we proposed method.

IV. PROPOSED SYSTEM FRAMEWORK AND DESIGN

A. Architecture

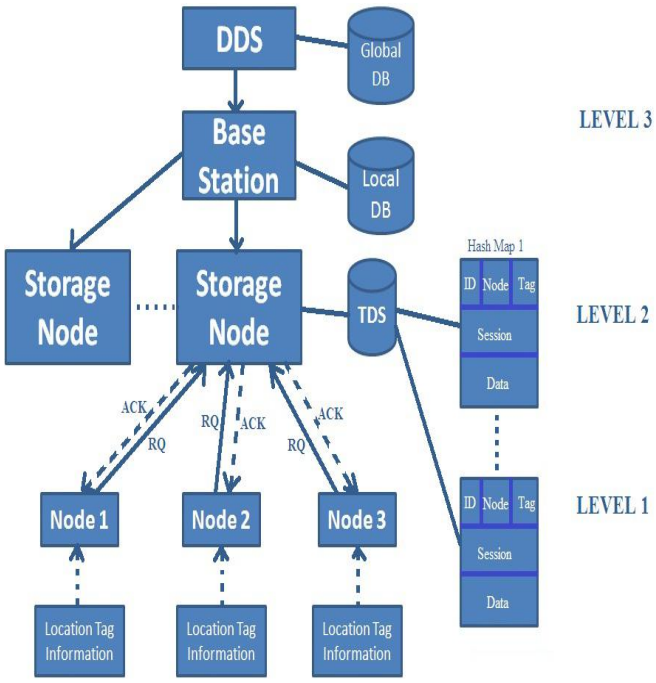

Fig.1: System Architecture

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 7, July 2015

B. Proposed Work

In proposed model, the aggregation is done by three different levels. The sensing node broadcasts the packet or message in the same session. The packet used for this purpose is UDP (User Datagram Packet). Structure of packet is shown in fig.2

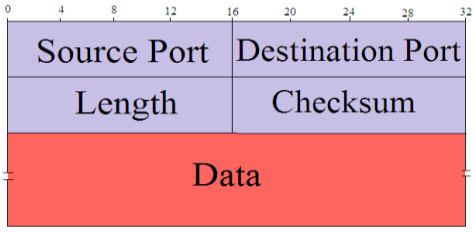

Fig. 2: Structure of Packet

The UDP header consists of 4 fields, each of which is 2 bytes (16 bits).

1.Source port number

This field identifies the sender's port when meaningful and should be assumed to be the port to reply to if needed. If not used, then it should be zero. If the source host is the client, the port number is likely to be an ephemeral port number. If the source host is the server, the port number is likely to be a well-known port number.

2. Destination port number

This field identifies the receiver's port and is required. Similar to source port number, if the client is the destination host then the port number will likely be an ephemeral port number and if the destination host is the server then the port number will likely be a well-known port number.

3. Length

A field that specifies the length in bytes of the UDP header and UDP data. The minimum length is 8 bytes since that's the length of the header.

4. Checksum

The checksum field is used for error-checking of the header *and* data. If no checksum is generated by the transmitter, the field uses the value all-zeros. This field is not optional for IPv6.

In Level 1, Sensing node and storage nodes are present. In Level 2, number of Base station are present and in Level 3 which is the uppermost level, only one DDS is present which manages the whole hierarchy of the network. With the help of location tags we are going to form a secure communication. Location tag of each node will be different. There are two location tags i.e. Public location tag and secret location tag. Public location tag unites RSSI, MAC addresses and sequence number to identify packet whereas secret tags knows only packet arrival time information and kept by the client. On the basis of these location tags, signature will be created which will be useful for the session key establishment. Our signature will be the combination of Session key and location tag. Session key will be based on timestamp also. Hash table is present in the architecture, which will store all the information or we can say tag information.

The proposed algorithm for data aggregation and session key generation and each detailing of techniques are described in section 3.C.

C. Algorithms

Algorithm 1: For Data Aggregation

Level 1

If (S is Secure)

then, combine all sensor data

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 7, July 2015

from its own region
End if

Level 2
If(S€Sn)
then, check present sessionId
if(sessionId not present)
then create new data set
End if

Level 3
If(not)
Check that data present in TDS
or not
Check if same sessionId
Else
Forward data to nearest Base
station
Entry to TDS
Session encrypt data
Add sessionId
Apply signature on it

Algorithm 2: For Session Key Generation

Input: $A=[A_i]$
$Z=[Z_i]$
t_i^A and t_i^Z packet arrival time
t_a= arrival time of reference packet
r= rounding precision
Output: Session keys K_A and K_z
T= Timestamp
I ← {0≤I, j≤N, $A_i = Z_j$}
J ← {0≤I, j≤N, $A_i = Z_j$}
A sends J to Z
Timestamp of both A and Z are recorded
For i=1 to N
$T_i^A \leftarrow r(t_i^A - t_a, 10^{-r})$
$T_i^Z \leftarrow r(t_i^A - t_a, 10^{-r})$
End for
$K_A = [T_i^A]$, where i=1,2,…I
$K_Z = [T_i^Z]$, where i=1,2,…J
Signature(A)= $K_A + T_A$
Signature(Z)= $K_Z + T_Z$

D. Mathematical Model

System can be described mathematically. For mathematical model we consider S will describe total system. So S will be,

S = {Input, Output, Process}

Detail of each element is given below,

Input Sets:
Input = {Packets, Messages}

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 7, July 2015

Output Sets:

Output= {Location tags, Packets, Messages}

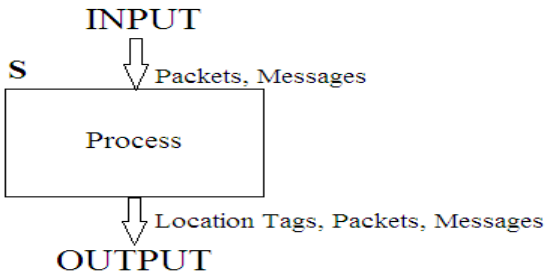

Fig.3 Illustration

Process:

1. Level 1

   In Level 1, all the storage nodes are present. In each storage node, there are number of sensing nodes present which will be going to broadcast message or packets.

   Let,

   N_n= Number of Sensing nodes

   S_n= Number of Storage nodes

   Thus, to represent Level 1, we can write as follows,

   $S_j = \sum N_i$

   Where i= 1,2,3….n

2. Level 2

   In Level 2, all the base stations are present. In each base station, there are number of storage nodes present which wil keep information of lower level i.e. Sensing nodes.

   Let,

   B_n= Number of Base station

   Thus, to represent Level 2, we can write as follows,

   $B_j = \sum S_i + \sum N_i$

   Where i= 1,2,3….n

3. Level 3

   In Level 3, only one Distributed data server (DDS) is present, which will have the whole information about all the lower levels. We can say that it will keep information of complete network.

   Let,

   D= Distributer data server

   Thus, to represent Level 3, we can write as follows,

   $D = \sum B_i + \sum S_i + \sum N_i$

   Where i= 1,2,3….n

4. Session key Generation

   In this, session key is generated which is going to applicable in all the three levels of network.

   A= Sender

   Z= Receiver

   $A_i = \{MAC_i^A, SN_i^A\}$

   $Z_i = \{MAC_i^Z, SN_i^Z\}$

   t= Packet arrival time

   K_A= Session key of A

   K_z = Session key of Z

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 7, July 2015

T_A = Timestamp of A
T_Z = Timestamp of Z

V. PRACTICAL RESULTS AND EVIRONMENT

In this section we are presenting practical environment, dataset used, and metrics computed.

A. Software Used

Software Configuration
- Operating System: Windows 7
- Programming Language: Java

B. Results

Input
1. Request from sender node.
2. Packets or Message to send.

Output

1. Location tags of node.
2. Detecting authenticated user and allow them to communicate securely.
3. Establishment of communication with session key.

Results

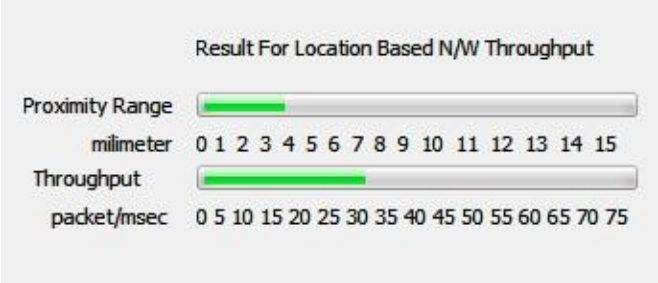

Fig 3: Result for location based network throughput

Proposed methods throughput will be less as compared to existing system. It will send more packets in less time. Result is plotted between proximity range and throughput. Proximity is nearness of the distance which will be sensed by nodes.

VI. CONCLUSION

Paper presents a good approach for detecting authenticated user from the wireless sensor network using location tags. We proposed a privacy preserved proximity based multilevel session aggregation system which is also is vigorous against spoofers and eavesdroppers outside the proximity range. System is location-based services in wireless networks, without requiring any public key infrastructure, trusted authority or early required secret. Secret location tags are not easily disclosed to anyone, so that more secure system is generated. In this system, the proximity based authentication and multi level session key establishment are implemented based on temporal location tags. Session key is generated in each level of network. Session key and location tags combinely form signature, which is also based on timestamp of packet arrival.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 7, July 2015

In results, we have shown that throughput of system can be minimized; also as we are using aggregated data which will compress packet and requires less space and so transmission time. Also we have compared total proximity time with estimated proximity time in results. and all above parameters are compared with proximity range.

ACKNOWLEDGEMENT

I would like to thank the anonymous referees for their helpful guidance that has improved the quality of this paper. Also I would like to thank my Project Guide Prof. S. S. Biradar, for his valuable guidance.

REFERENCES

[1] Liang Xiao, Qiben Yan, Wenjing Lou, Guiquan Chen, and Y. Thomas Hou, "Proximity-Based Security Techniques for Mobile Users in Wireless Networks" IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 8, NO. 12, DECEMBER 2013, 2098-2100
[2] A. Varshavsky, A. Scannell, A. LaMarca, and E. Lara, Amigo: Proximity-based authentication of mobile devices, in Proc. Int. Conf. Ubiquitous Comput., 2007, pp. 118
[3] Z. Zhu and G. Cao, Applaus: A privacy-preserving location proof updating system for location-based services, in Proc. IEEE INFOCOM, Apr. 2011, pp. 18891897.
[4] A. Kalamandeen, A. Scannell, E. de Lara, A. Sheth, and A. LaMarca, Ensemble: Cooperative proximity-based authentication, in Proc. ACM Int. Conf. Mobile Syst., Appl. Services, Jun. 2010, pp. 331344.
[5] A. Narayanan, N. Thiagarajan, M. Lakhani, M. Hamburg, and D. Boneh, Location privacy via private proximity testing, in Proc. NDSS, 2011, pp. 117.
[6] N. Talukder and S. Ahamed, Preventing multi-query attack in locationbased services, in Proc. 3rd ACM Int. Conf. Wireless Netw. Sec., 2010, pp. 2536.
[7] Suhas Mathur , Rob Miller, Alexander Varshavsky, Wade Trappe, and Narayan Mandayam, "ProxiMate: Proximity-based Secure Pairing using Ambient Wire- less Signals"
[8] Kumar PADMANABH, Sunil Kumar VUPPALA, "An Adaptive Data Aggregation Algorithm in Wireless Sensor Network with Bursty Source" Wireless Sensor Network, 2009, 3, 222-232

BIOGRAPHY

Chetna D. Salame Research Scholar RMD Sinhgad SOE Pune, University of Pune. She received B.E. in Computer Engineering from Bapurao Deshmukh Foundations Suresh Deshmukh College of Engineering, Selukate, Wardha from RTMNU. Currently she is persuing M.E. in Computer Engineering from RMD Sinhgad School Of Engineering Pune,University of Pune.

Shripadrao Biradar received the B.E. degree in Computer Science and Engineering from PDACOE Gulbarga Karnataka and M.E. degree in DCN from Dr. AIT Banglore Karnataka in 2010 and 2012 respectively. Currently he is working as Assistant Professor of Computer Engineering Department in RMDSSOE Pune, India.