International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

A Survey Paper of Proximity-Based Security Techniques for Mobile Users in Wireless Networks Multi Level Location Based Session Aggregator

Shripadrao Biradar[1], Chetna Salame[2]

[1]Professor, Department of Computer Engineering, RMD Sinhgad School of Engineering, University of Pune, India

[2]Department of Computer Engineering, RMD Sinhgad School of Engineering, University of Pune, India

Abstract: ***In this system, the proximity based authentication and multi level session key establishment are implemented based on spatial temporal location tags. Constituting the unique physical features of the signals sent from multiple ambient radio sources, the attacker cannot easily forged the location tags. More specifically, each radio DDS builds a public location tag according to the received signal sequence numbers, strength indicators and media access control (MAC) addresses of the ambient packets. Each DDS also keeps a secret location tag that consists of the packet arrival time information to generate the multi level session keys. As DDSs never disclose their secret location tags and this system is robust against spoofers and eavesdroppers outside the proximity range.***

Keywords: Authentication, encryption, wireless networks, Gaussian mixture model.

1. Introduction

We propose a privacy-preserving proximity-based security system for location-based services in wireless networks which do not require any trusted authority, pre-shared secret, or public key infrastructure. Incorporating the unique physical features of the signals sent from multiple ambient radio sources, the attacker cannot easily forged the location tags. More specifically, each radio DDS builds a public location tag according to the received signal sequence numbers, strength indicators, and media access control (MAC) addresses of the ambient packets. Each DDS also keeps a secret location tag that consists of the packet arrival time information to generate the multi level session keys. As DDSs never disclose their secret location tag and this system is robust against spoofers and eavesdroppers outside the proximity range. The authentication accuracy of the system is improved by introducing a nonparametric Bayesian method called infinite Gaussian mixture model in the proximity test and provides flexible proximity range control by taking into account multiple physical-layer features of various ambient radio sources. Moreover, the multi level session key establishment strategy significantly increases the key generation rate by exploiting the packet arrival time of the ambient signals. The key generation rate and authentication accuracy are evaluated via experiments using laptops in typical indoor environments.

2. Proposed Work

2.1 Problem Statement

Proximity-Based Security Techniques for Mobile Users in Wireless Networks

2.2 Multi Level Location Based Session Aggregator for Security

a) Level-1
The proximity-based authentication is based on the similarity between the physical features of the shared ambient radio signals obtained by the radio DDSs. More specifically, Source compares her trace with Destination's measurements extracted from his public location tag, according to a nonparametric Bayesian method (NPB) called infinite Gaussian mixture model (IGMM). Unlike the hypothesis tests such as maximum likelihood estimation, IGMM does not rely on the *a priori* knowledge of the input data model and works well even with uncertainty regarding the number of hidden classes and the data model in Level 1.Whenever the receiver node receives its children readings or any request from the source node S, it computes to identify whether it processes the request or not by Is Secure algorithm. At first, it checks the data is receiving from its own

b) Level-2
During the aggregation process for the middle and above (level 2 and level 3), it checks not only the data duplication alone but also considered the closer data set. Here a threshold value (δ) is used for measuring the very closer data set which belongs to the received the data

c) Level-3
In higher level data aggregation, the base stations combine all sensors data received from storage nodes or from sensor nodes from its own region when the source node (S) is secure.

2.3 Objective

The goal of this project is to provide secure communications, such as authentication, confidentiality, duplication, data integrity and service availability for mobile user in WSN

Advantage

1. To Support secure communications among the users in mobile network.
2. In Layer-management scheme, which scales logarithmically with network size O (log n), with respect to storage space.
3 .without involving any trusted authority, pre-shared secret or public key infrastructure
4. PHY-layer security strategy with the existing traditional security protocols to address the man-in-the-middle attacks inside the proximity.

2.4 Existing System

In secure communication, WSN uses symmetric key techniques. Secret keys are redistributed among nodes in symmetric key techniques before their deployment. The main challenge of the key distribution scheme is to use small memory size to establish secure communication among a large number of nodes and achieve good resilience. Public-key MAC Location based approaches were originally proposed to provide solutions to secure communications for the mobile network, where security services rely on a centralized MAC Location server. The MAC Location-based approaches to mobile networks and present a distributed public-key-management scheme for WSN networks, where multiple distributed MAC Location authorities are used. To sign a MAC Location, each authority generates a partial signature for the MAC Location submits the partial signature to a coordinator that calculates the signature from the partial signatures.

Disadvantage

1. Lack of support for authentication and confidentiality.
2. Whose location tag incorporates the contents of the ambient packets, this strategy depends on the physical-layer features,
3. Total number of keys held by each user is O (n) traditional key-management schemes

3. Conclusion

We have proposed a proximity-based authentication and key establishment scheme by exploiting the physical-layer features of ambient radio signals for LBS services in wireless networks, which do not require any pre-shared secret. Flexible range control is achieved by selecting the appropriate radio sources, such as ambient WiFi access points (APs), bluetooth devices and FM radios and choosing their suitable physical-layer features.

The system applies the Markov chain Monte Carlo implementation of the infinite Gaussian mixture model (IGMM) to classify the RSSIs of multiple ambient signals and thus determines whether a client is in the proximity.

The system does not disclose the client locations, and is robust against eavesdropping, spoofing, replay attacks and man-in-the-middle attacks outside the proximity. By applying the IGMM model, the authentication is more accurate and is less sensitive to the radio propagation pattern than existing RSS and CIR-based authentication strategies. The key generation rate that can be as high as 248 bps in ideal cases is much higher than that of the RSSbased strategies. In the future, we will further evaluate the performance of the proposed strategy with experiments based on FM, Bluetooth and WiFi ambient signals and study how to incorporate this PHY-layer security strategy with the existing traditional security protocols to address the man-in-the-middle attacks inside the proximity.

References

[1] M. Li, W. Lou, and K. Ren, “Data security and privacy in wireless body area networks,” *IEEE Wireless Communication.*, pp. 51–58, Feb. 2010, vol. 17, no. 2.
[2] X. Liang, R. Lu, C. Le, X. Lin, and X. Shen, “PEC: A privacy-preserving emergency call scheme for mobile healthcare social networks,” *J. Communication. Network.*, pp. 102–112, Apr. 2011, vol. 13, no. 2.
[3] Z. Lin, N. Hopper and D. Kune, “Efficient private proximity testing with GSM location sketches” (Lecture Notes in Computer Science) New York, NY, USA: Springer-Verlag, 2012, pp. 73–88.
[4] I. Martinovic, M. Strohmeier,, S. Eberz and M. Wilhelm “A practical man-in-the-middle attack on signal-based key generation protocols,” in *Proc. ESORICS*, 2012, pp. 235–252.
[5] H. Sasaoka, T. Aono, T. Ohira, B. Komiyama, and K. Higuchi “Wireless secret key generation exploiting reactance-domain scalar response of multipath fading channels,” *IEEE Transaction Antennas Propagation*, pp. 3776–3784, Nov. 2005, vol. 53, no. 11.
[6] L. Xiao, L. Greenstein, N. B. Mandayam, and W. Trappe, “Channelbased spoofing detection in frequency-selective Rayleigh channels” pp. 5948– 5956, Dec. 2009, vol. 8, no. 12.” IEEE *Transactions. Wireless Communication.*
[7] A. Varshavsky, A. LaMarca, E. Lara and A. Scannell, “Amigo: Proximity-based authentication of mobile devices,” in *Proc. Int. Conf. Ubiquitous Computation.*, 2007, pp. 1–18.
[8] A. Reznik,, , C. Ye, S. Mathur, W. Trappe and N. Mandayam “Radiotelepathy: Extracting a secret key from an unauthenticated wireless channel,” in *Proc. ACM 14th Annual Conference Mobile Computation. System.*, 2008, pp. 128–139.
[9] C. Rasmussen, “The infinite Gaussian mixture model” in *Advances in Neural Information Processing Systems*. Cambridge, MA, USA: MIT Press, 2000, pp. 554–560.

Author Profile

S. S. Biradar received the B.E. Degree in Computer Science & Engineering from PDACOE Gulbarga Karnataka & M.E. degree in DC&N from Dr AIT Banglore Karnataka in 2010 & 2012 , respectively. Currently he is working as Assistant Professor of Computer Engineering Department in RMD SSOE Pune, India.

Chetna D. Salame is Research Scholar RMD Sinhgad SOE Pune, University of Pune. She received B.E. in Computer Engineering from Bapurao Deshmukh Foundation’s 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, Pune, Maharashtra, India