NICE TO MEET YOU AGAIN: FRIENDS' AUTHENTICATION FOR MOBILE OBJECTS.

Kim Khanh T. Tran*
Faculty of Computer Science and Engineering, Ho Chi Minh University of Technology
Ho Chi Minh, Viet Nam
ttkkhanh@ctuet.edu.vn

Fabio Massacci
DISI - University of Trento
Trento, Italy
fabio.massacci@unitn.it

Giampietro Picco
DISI - University of Trento
Trento, Italy
gianpietro.picco@unitn.it

Tran Khanh Dang
Faculty of Computer Science and Engineering, Ho Chi Minh University of Technology
Ho Chi Minh, Viet Nam

ABSTRACT

So far, there are so many ways to authenticate users through biometrics, password-based or token/smart card, world trends are developing the advantage of wireless sensor networks that enables a flexible approach to verifying. Besides, user's device is constrained including energy, memory and bandwidth Some previous works had ideas based on those conditions that serve different purposes and contexts. In this article, we propose a mechanism to keep the last encounters alive for a certain period of time or a trust limit, along with creating new links based on make a security interaction by friends. Finally, we implement the protocol through a simulation application which represents the average number of former and latter links chronologically to track the process of updating the association in time and trust levels to make the right choice for the practical application.

CCS CONCEPTS

• **Networks** → Network security;

KEYWORDS

Mobility Hepls, Algorithm, Time of Encounters, Wireless Sensor Network

1 INTRODUCTION

-tbc-

2 HIGH-LEVEL MECHANISM

2.1 System Model and Assumptions

Before describing our technique, they will supply a system model and the hypothesis of applying our technique.

We consider in the wireless sensor network as well as appropriate for the IoT application, so the nodes represent the smart sensors as a user with a smart mobile device (phone, tablet, pen or watch) or an mobility object. Our model will not involve the central authority, no central servers or the fixed base-station. They can communicate with each other through the wireless technologies such as bluetooth, zigbee, etc. The signal transmission range of these technologies is very short and the bandwidth is also lower than the technology used for high power devices such as Wi-fi, Dect, ...

Each node will be able to locate itself via GPS, so that it can identify neighbors around it. In addition, they store a list of devices which they are aware of the proximity, the list will contain: ID and time of encounter. The wireless network will be set up based on the above conditions, the nodes also have the small memory spaces, and a limited battery life.

We assume that the nodes were able to authenticate and establish an earlier secure link through a common friend approach [4,12]. In addition, the nodes can still perform this technique when in offline mode, only to be identified through the wireless technologies outlined above. We will focus on expansion and supplement to the old protocol [4,12] as discussed in Introduction section, we offer to make the protocol more flexible in the case of last encounters and add a trust value to increase the reliability of new node encounters.

In our mechanism, we will introduce three main roles that will be involved: the claimant, the verifier and the certifier, where the claimant is a node want to make a security link with the certifier and the verifier will a node that helps the claimant to identity. In addition, we assume that this extended mechanism is an one-way establishing.

2.2 Evolving Broadcast Authentication Scheme

We consider the following scenario: When a relationship is established, each person adds another to the their list, which is considered to be an established relationship, as a friendship. Using friend-assisted establishment protocol, ID of friend, time of encounter, a random number and public-key of friend included in each node's list. We will succinctly describe each step of the scheme and specify the step that we apply our mechanism to modify the scheme.

Joining : When a stranger as Alice moves to a particular area, he will catch the proximity nodes which belong to this area, we observe two case which will happen in this step.

(1) The old friend: Alice will prove her triplet to the nearest friend by broadcast to access the services of area.
(2) The stranger/ new neighbor: Alice is a stranger with the nearest nodes as David, Ellen, etc. Alice sent a request to David to make a association.

*this author is also a staff of Faculty of Information Technology, Can Tho University of Technology, Can Tho, Viet Nam

Authentication Session: The previous works proposed mechanisms to build a new secure connection by exchange security material, friend-assisted helps. However, this old interaction is no longer trusted, the interactive node is likely to have been compromised or it is an intermediate node in a collusion attack. Following the above cases,this session is also divided two different ways to authenticate.

(1) The old friend: Alice has already had a security association with the nearest nodes as Bob, Charlie, David, etc. If the interval from establishing the interaction to reuniting is not greater than Δ_{time}, the mechanism will update this interaction by update the public-key and time of encouters.
(2) The stranger/ new neighbor: David check and broadcast the Alice's request to some close friend (based on David's power and signal) about Alice's status. If someone knew Alice and the interval they have not meet each other is also not greater than Δ_{time}, they will commit their material and Alice's public key to verify Alice's identity. We will append the trust value as Δ_{trust}, to compute with those responses.

After the authentication period, the new relationship is established or the interaction is kept alive with the new material included new public-key, new value of time in a secure channel.

3 MECHANISM FOR UPDATING ASSOCIATION ON TIME/TRUST

-tbc-

4 PERFORMANCE

-tbc-

5 RELATED WORK

-tbc-

6 CONCLUSIONS

-tbc-

REFERENCES

[1] Brainard J., Juels A., Rivest R. L., Szydlo M., Yung M. . "Fourth-factor authentication: somebody you know." In *Proceedings of the 13th ACM conference on Computer and communications security*, pp. 168-178. ACM, 2006.
[2] Callaway Jr and Edgar H. "Wireless sensor networks: architectures and protocols." *CRC press*, 2003.
[3] Rashid B. and Mubashir H. R. "Applications of wireless sensor networks for urban areas: A survey." *Journal of Network and Computer Applications 60* (2016): 192-219.
[4] ÄŇapkun S., Jean-Pierre H. and Levente B. "Mobility helps security in ad hoc networks." *Proceedings of the 4th ACM international symposium on Mobile ad hoc networking & computing*, 2003.
[5] Virendra M., Jadliwala M., Chandrasekaran M. Upadhyaya S. "Quantifying trust in mobile ad-hoc networks." *Integration of Knowledge Intensive Multi-Agent Systems* 2005. International Conference on. IEEE, 2005.
[6] Nadeem A., Javed, M. Y. "A performance comparison of data encryption algorithms."*In Information and communication technologies*, pp. 84-89, 2005
[7] Agrawal M., Mishra P. "A comparative survey on symmetric key encryption techniques" *International Journal on Computer Science and Engineering* 4(5), 877,2012.
[8] Chan H., Perrig A. "PIKE: Peer intermediaries for key establishment in sensor networks" *24th Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings IEEE*,Vol. 1, pp. 524-535,2005.
[9] Zhang Y., Liu W., Lou W., Fang Y. "Location-based compromise-tolerant security mechanisms for wireless sensor networks" *IEEE Journal on selected areas in communications* 24(2), 247-260,2006.
[10] Karlof C., Sastry N., Wagner D. "TinySec: a link layer security architecture for wireless sensor networks." In Proceedings of the 2nd international conference on Embedded networked sensor systems (pp. 162-175). ACM. 2004.
[11] Chang S. M., Shieh S., Lin W. W., Hsieh C. M."An Efficient Broadcast Authentication Scheme in Wireless Sensor Networks" Proc. 2006 ACM Symp. Information, Computer and Communications Security (ASIACCSâĂŹ06),2006.
[12] Capkun S., Hubaux J. P., Buttyan L. "Mobility helps peer-to-peer security." *IEEE Transactions on Mobile Computing*, 5(1), 43-51. 2006.
[13] Velloso P. B., Laufer R. P., Cunha D. D. O., Duarte O. C. M., Pujolle G. "Trust management in mobile ad hoc networks using a scalable maturity-based model."*IEEE transactions on network and service management* 7(3), 172-185.2010.
[14] Perrig A, Szewczyk R, Tygar JD, Wen V, Culler DE., "SPINS: Security Protocols for Sensor Networks".*Wireless Networks* vol. 8, no. 5,pp.521âĂŞ34. 2002
[15] Liu D., Ning P. "Efficient Distribution of Key Chain Commitments for Broadcast Authentication Distributed Sensor Networks," *Proc. 10th Annual Network and Distributed System Security Symp.*, San Diego, CA. pp. 263âĂŞ76.2003.
[16]]Liu D., Ning P. "Multilevel μTESLA: Broadcast authentication for distributed sensor networks." *ACM Transactions on Embedded Computing Systems (TECS)*, 3(4), 800-836.2004.