Trust-Propagation Based Authentication Protocol in Multihop Wireless Home Networks

Han Sang Kim, Jin Wook Lee*, Sandeep K. S. Gupta and Yann-Hang Lee
Department of Computer Science and Engineering
Arizona State University
Tempe, Arizona 85287
{hanskim, sandeep.gupta and yhlee}@asu.edu,
*Communication Lab.
Samsung Advanced Institute of Technology (SAIT)
Yong Shi, Republic of Korea
thetruth.lee@samsung.com

***Abstract*— In this paper, we propose an authentication and secure channel establishment protocol that is reliable and adaptable for multihop wireless home networks. The main idea is that a home server hands over its authenticating capability to some already authenticated devices to enable these devices to be able to authenticate other devices which cannot reach the home server directly due to their physical location and radio power constraints. Key to our design is a neighbor device authentication protocol, based on pre-user-injected network password, with minimal reliance on public key cryptographic operation. In addition, our protocol supports a secure channel establishment among heterogeneous devices after authentication. Through the evaluation, we show that our protocol is resistant to various attacks.**

***Index Terms*— Security, Authentication, Wireless Multi-hop home Network.**

I. Introduction

IN the future, homes will use multihop wireless networks to connect all the devices to one another. Multihop wireless technology could solve a number of limitations that extend beyond simply eliminating dead zones in home. Depending upon the data rate (bandwidth) requirement different wireless technologies can be employed. For example, emerging wireless standards such as Zigbee (IEEE 802.15.4) [1] are suitable for many home automation and personal healtcare applications which require low data rate. Zigbee is optimized for prolonged battery-powered operation. Due to short range (about 15m in a cluttered office/home environment) of a single Zigbee device, it supports (and requires) multihop routing to increase coverage of a Zigbee network. To satisfy the demands of the digital home with high-speed data rates, Bluetooth scatternets [3], multihop WiFi networks [2] and Mesh networks [4] can be used.

Wireless home networks require a robust authentication mechanism due to the accessibility to the devices, the heterogeneity of communication protocols and the wireless environment. Our authentication protocol relies on a home server to propagate authentication to the network. In a common home networking environment, a server-based approach is more advantageous, as we can impose most of the cost/complexity on the home server. In this paper, we suggest a way to efficiently authenticate home devices using trust-propagation in multihop wireless home networks. The fundamental idea of the proposed authentication protocol is that a home server hands over authentication privilege to the already authenticated devices. Eventually all the devices in the network are authenticated and then become authenticators on behalf of the home server. Our protocol achieves low communication cost and scalability by allowing multihop peer-to-peer communication of devices.

The rest of the paper is organized as follows: Section II describes our system model, assumptions and design goals. In section III, we propose our trust-propagation based authentication protocol. In section IV, we presents the security analysis of our protocol. Finally, we conclude this work in section V.

II. The Approach

A. System Model and Assumptions

Our system model consists of a home server and multiple home devices, such as TV, home theater system, and PDA. Locations of devices are dynamic but we assume that the mobility of devices is limited within the confines of a home. The first device activation is done by an user by inputting a memorizable password. For instance, when a user buys a home network device and enters a password agreed with the home server. This assumption is reasonable because unexpected home devices should not be participating in the home network. We assume that home devices have limited radio transmission power so a multihop network should be installed at home in near future. Since many of the devices in the network may be battery-powered, our design goal is to make the authentication protocol as efficient as possible in terms of communication overhead, i.e. minimize number of messages exchanges, as well as computation overhead, i.e. minimize number of (possibly expensive) public-key cryptography operations.

B. Definitions

We here briefly introduce two key concepts of our protocol.

- **Badge**: A badge is similar to the concept of digital signatures in terms of the properties such as its unforgeability,

verifiability, unreuseability, and undeniability. It is used for determining whether authority for authentication belongs to an individual node. This is in contrast to using it for verifying whether a public key belongs to an individual. Specifically, in our proposed protocol, *Badge* is used by a home server to delegate only its authenticating capability to an already authenticated device. Upon possessing a badge, an authenticated device can authenticate other devices on behalf of the home server. Note that the server gives a device only limited authority, i.e. authentication authority.

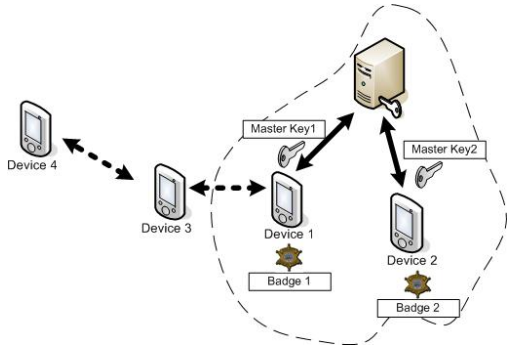

Fig. 1. One hop Authentication Domain

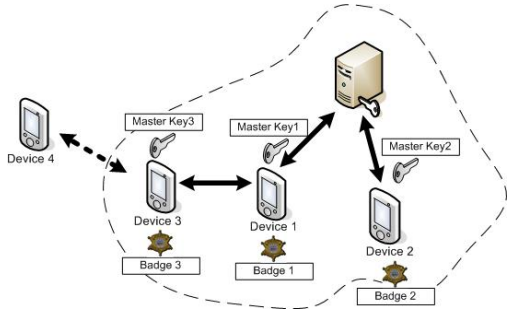

Fig. 2. Multi hop Authentication Domain with Trust Propagation

- **Authentication Domain**: When a user wants to introduce a new device D to be used in an existing home network, the device needs to be authenticated by the home server S of the network. According to our system model, it is not guaranteed that the the new device is located in the radio range of a home server. In case D is out of range of S, it tries to be connected to other authenticated devices to securely reach S. We define *Authentication Domain (AD)* as a group of authenticated devices. Every home network has just one authentication domain. Each device in a AD is allowed to communicate with other devices in the AD using a secure channel. Specifically, all nodes that have same *Badge* are part of the authentication domain $AD(Badge)$. Figure II-B shows an example of Authentication Domain.

III. Trust-Propagation Based Authentication Protocol

Once a new device D is initiated to be added to the user's home network by being provided with the password, it broadcasts a beacon message (also called hello message) to discover the home server S or other already authenticated devices and to try to be authenticated. Following are the four possible responses the new device could expect in response to its beacon message:

- ***Server response***: If the home server receives the beacon message from a new device, the server responds to let the device start the Authentication Process.
- ***Neighbor response with Badge***: If one of the neighbor devices who has a *Badge*, this already authenticated device could respond to the new device's request message. The new device starts the Authentication Process with the neighbor device.
- ***Neighbor response without Badge***: In case no neighbor device has the *Badge*. The beacon message is periodically broadcasted to allow the device to probe other devices.
- ***No response***: There is no neighbor device in the radio range of the new device. In this case, the new device is isolated in the network. In order to get connected to the home network, the new device should be moved into a location from where the device can reach some other devices in the network.

Only the home server can generate a *Badge* and grant it to a device, even though the device is authenticated by one of its neighboring devices. For ease of understanding, we list the notations used in the paper in Table I.

TABLE I
Glossary

Notation	Description
ID_X	Identity of device X
$npwd$	Initial shared network password for device checking
K_X	X's master key which is only shared with a home server
K_{XY}	Session key for X and Y, shared key between X and Y
R_X	A random nonce generated by X
TS	Timestamp
L	Life time of a key or *Badge*
ATH	Uses of the *Badge*. The Badge could be used for various uses according to this limited authority
$REP(X)$	Report message about authentication of device X
$RQA(X)$	Request message of access to device X
ALG	An algorithm indicated by a home server

Our proposed protocol consists of two main phases. The initial authentication phase is followed by the expanded authentication phase. As mentioned earlier, our authentication process is initiated by the password agreement. At this time, we assume all devices have the same password in the hardware at the start of the protocol.

A. Initial Authentication Phase: Phase I

Neighbor devices of the home server get securely authenticated by the four protocol packet exchanges as shown in Fig-

ure 3.

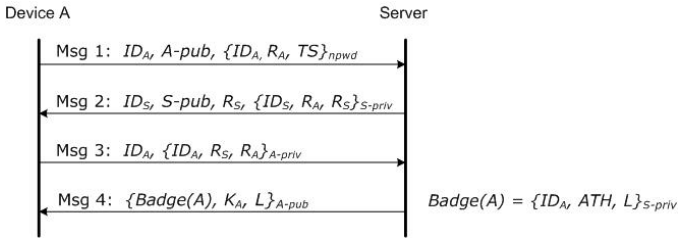

Fig. 3. Authentication in one hop from the server

In most of the proposed authentication protocols so far, it has been assumed that the shared secret key is manually distributed and typed, and then authentication protocol and key distribution are built on this assumption. In a home network, it is unreasonable to expect a network user (a family member) to type a long shared secret key to every device. It is also unreasonable to assume that every device is physically connected to the home server. Therefore, we use a simple password-based scheme. Before a device is used for the first time in a home network, a user manually enters a network password (shared secret) in the device as its only network authentication key. This network password is a weak human-memorizable password because of it's limited length. It is only used for verifying if the device is user's network device. We discuss the proposed protocol by describing the packet exchange one by one. We define nine protocol packets represented by [Msg *number*].

After bootstrap, any device broadcasts hello message to announce its presence. If there is an authenticated device including the home server, the device informs unauthenticated neighbor devices. An unauthenticated device, device A, sends Msg 1 to the home server, S as below.

[Msg 1] A $\Rightarrow$ S : ID_A, *A-pub*, $\{ID_A, R_A, TS\}_{npwd}$

Device A generates a large random number R_A as a challenge, and then unicasts the random number and time stamp TS encrypted with a network password, its identity and public key. At manufacture time, each device is given a public/private key pair certified by the manufacturer in tamper resistant memory. When the home server receives Msg 1, it decrypts the message with the network password the user registered. The home server S confirms the freshness of the message (to prevent replay-attack by an adversary) by examining the decrypted time stamp.

[Msg 2] S $\Rightarrow$ A : ID_S, *S-pub*, R_S, $\{ID_S, R_A, R_S\}_{S\_priv}$

After checking the time stamp, the home server sends device A back a message containing the random number (R_A) encrypted with the network password and its own random number (R_S) as a challenge (Refer to Msg 2 above). When device A gets Msg 2, it uses the server's public key S$-$pub to decrypt the last argument of the message to obtain R_A and R_S. The message must have come from the home server, since a malicious device is not able to determine R_A and encrypt it with the server's private key. Furthermore, it must be fresh and not be a replay since device A just broadcasted R_A.

[Msg 3] A $\Rightarrow$ S : ID_A, $\{ID_A, R_S, R_A\}_{A\_priv}$

After having received Msg 2, device A sends the server back a message encrypted with its own private key containing the random number from the server and its own random number. When the server decrypts Msg 3 with device A's public key and retrieves the two random numbers, the server authenticates that the remote device is actually the device A.

[Msg 4] S $\Rightarrow$ A : $\{Badge(A), K_A, L\}_{A\_pub}$
$Badge(A) = \{ID_A, ATH, L\}_{S\_priv}$

Through Msg 1 to 3, not only does the server authenticates device A but device A also authenticates the home server (mutual authentication). After the device A becomes aware of a part of the network, the home server gives device A *Badge* and a master key which is only shared between the home server and device A so that it will be used for the remainder secure connection with the server instead of using the asymmetric key. The *Badge* is a certificate signed and issued by the server as was described in an earlier section. It gives device A a permission to authenticate other devices in its neighborhood on behalf of the server whenever those devices cannot directly perform authentication procedure with the server due to their physical distance from the server. In other words, if a home server puts another device D's identity instead of A's identity in a *Badge*, it means that the server has allowed the device D to act as the server for authentication purpose.

B. Expanded Authentication Phase: Phase II

A device physically located where it cannot directly reach a home server tries to get authenticated by the aid of an already authenticated neighboring device with authentication authority. The procedure requires devices' relaying messages to the home server as shown in Figure 4.

During Hello message exchange, device B is informed from device A that device A is already authenticated by a home server. But device B still needs to verify the claim of device A. First, device B sends Msg 1 to device A.

[Msg 1] B $\Rightarrow$ A : ID_B, *B-pub*, $\{ID_B, R_B, TS\}_{npwd}$

Suppose that device A is previously assigned *Badge* and a master key by the server in *Phase I*, and device B is two hops away from the server. The neighbor device A, which is in the radio range of a device B, sends back a response to the challenge of a device A with Msg 5.

[Msg 5]
A $\Rightarrow$ B : ID_A, *S-pub*, R_A, $\{ID_A, R_B, R_A, Badge(A)\}_{B\_pub}$

This response message includes *Badge* assigned by the server. This message notably claims that device A is authorized by a home server and has a permission to authenticate other device with Badge. When device B gets Msg 5, device B can easily verify that not only *Badge* was issued by the server since it is encrypted by the server's private key, but also the server gave device A authority to authenticate others since *Badge* includes device A's identity and the authority of authentication.

[Msg 3] B $\Rightarrow$ A : ID_B, $\{ID_B, R_A, R_B\}_{B\_priv}$

After verifying the *Badge* sent from device A, device B sends a response to device A in Msg 3. Of course, device B discards

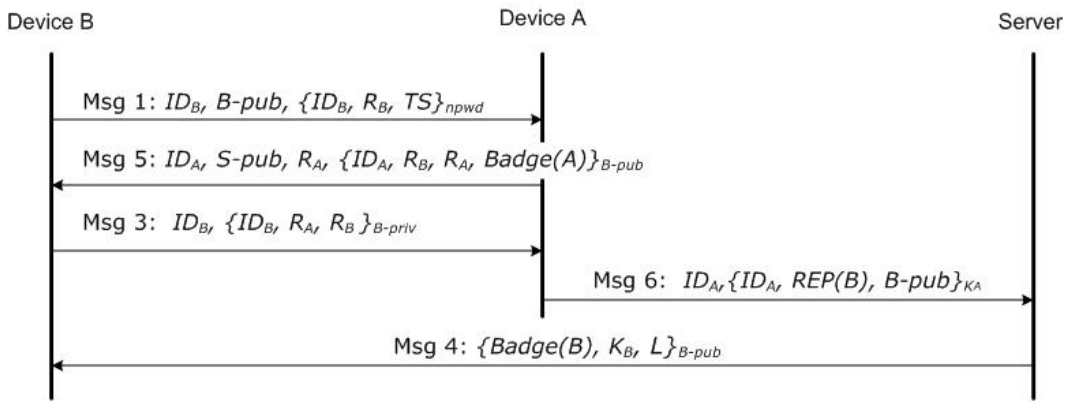

Fig. 4. Authentication in more than one hop from the server

Msg 5 if there is no *Badge* in it or *Badge* is not issued by the server.

[Msg 6] A $\Rightarrow$ S : $ID_A, \{ID_A, REP(B), B\text{-}pub\}_{K_A}$

Authentication of device B is performed by neighbor device A through Msg 1 to 3. After the authentication of device B, device A reports the fact to the server in Msg 6. $REP(B)$ is the report message. Msg 6 is encrypted with the master key. Note that the purpose of the master key is to enable the use of symmetric cryptography for encryption/decryption instead of asymmetric cryptographic technique, which consume more processing resources. Hence, any communication message between a server and a device is encrypted using the master key after the master key has been assigned.

[Msg 4] S $\Rightarrow$ B : $\{Badge(B), K_B, L\}_{B\_pub}$

After receiving Msg 6 from device A, the server generates a master key and makes *Badge* for device B, and then sends device B Msg 4 encrypted with device B's public key which was informed by device A in Msg 6. As a consequence, the trust is propagated two hops away from the server. In a similar manner, trust can be propagated multiple hops away from the server.

C. Security Access Control for Device Communication

A primary concern in home networks is access control, the specification of how home network devices are allowed to interact with one another. The devices in an Authentication Domain are all networked with a home server through each master key. For security purpose, however, they should be still have only limited access to other devices in the domain. In other words, even though a device belongs to the domain after being authenticated, the device access must be controlled by the home server in regards to what modes of accesses it is allowed to perform on other devices. This access control is managed by the home server based on an access control list which is an array of entries with the following format:

- *subject*: an identifier of the device in Authenticated Domain
- *authorization*: an indicator of the rights being granted to the subject
- *security level*: for security services, a secure level of device categorized by a server. It is based on the capability and security service required by the device.

Once a device is part of the Authentication Domain, which means *Badge* and a master key has been given to the device, the device is able to access the home server through the master key. Whenever a device wants to establish a secure connection with another device it contacts the home server and follows the protocol as shown in Figure 5. The device sends an access request (Refer to Msg 7) to the home server. Second, the server checks the access control list and distributes a session key to the involved devices separately, which will be used for end-to-end communication between the two devices. The length of this key and algorithm for the communication is decided according to the security level of access control list in the server. The goal of access control constrained by a security level is to provide appropriate access/service for heterogeneous home devices.

[Msg 7] B $\Rightarrow$ S : $ID_B, \{ID_B, RQA(C)\}_{K_B}$

Suppose that a device B and C are in an Authentication Domain, which implies that each of them has its own master key and *Badge*. Whenever device B wants to establish secure channel with device C, it sends the server a request access message ($RQA(C)$) encrypted by its master key. The server checks the access right in the access control list. If device B has the access right of the device C, the server generates a session key, K_{BC}, and then sends it to the both parties separately using the following device specific Msg 8:

[Msg 8] S $\Rightarrow$ B : $\{ALG, K_{BC}, L\}_{K_B}$
[Msg 8] S $\Rightarrow$ C : $\{ALG, K_{BC}, L\}_{K_C}$

This session key is used not only for confidential data transmission but also message origin authentication during secure communication. That is, any message encrypted with the session key after the authentication is believed to originate from the peer principal who holds the session key. When the server distributes the session key, the server assigns the appropriate length of the session key which depends on the capability of a device, and also lets devices have a choice for an appropriate encryption algorithm, which will be used for encrypting/decrypting communication message between devices. In home networks, this session key length-agile and algorithm-agile technique [5] [6] is useful for device communication session since various traditional computing and embedded Internet

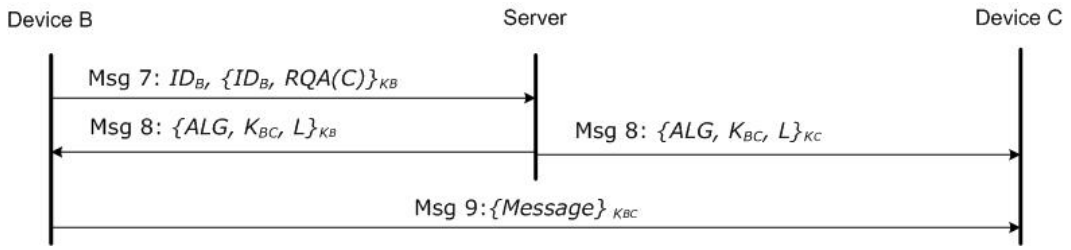

Fig. 5. Establishment of a secure connection with another device

devices can be networked. Different applications of heterogeneous devices need different security requirement for communication sessions with one another since certain devices may take a long time to encrypt/decrypt messages in each session. After the setup, device B could send device C data messages encrypted with the assigned session key.

[Msg 9] B $\Rightarrow$ C : $\{Message\}_{K_{BC}}$

IV. Evaluation

A. Security Analysis

Man-in-the-middle attack: The adversary intercepts the messages between the parties (a device and the server) and replaces them with its own messages. It plays the role of the device in the messages it sends to the server and at the same time plays the role of the server in the messages that it sends to the device.

Prevention: When a device which is more than one hop away from the server broadcasts a random number and a timestamp encrypted with a network password, its identity and its public key, an adversary puts himself between the parties on the communication line where it is one hop from the server. The parties would end up knowing the adversary's public key as a server's or the same home network device's. However, assuming that the network password has not been guessed or compromised, the adversary has no way to construct the encrypted message with a network password, so it is forced to resend $\{ID_A, R_A, TS\}_{npwd}$ with it's own identity and public key. When the server receives this message from the adversary, the server discards it since the decrypted identity with the network password does not match the identity which the adversary sends. Note that in case, the adversary tries to use the device's identity, this would be detected if the device continues to passively hear other on-going transmissions while the authentication process is not completed. If a device overhears a transmission with its own identity being used, it can alert the user in device-dependent manner that an intruder has been detected.

Badge reuse attack: The Badge is transmitted in the following two cases. One is when a server grants a device a Badge after authentication. The other is when an authorized device, which has a Badge, sends it to the device in unauthenticated domain for authenticating on behalf of a server. The adversary intercepts the message which includes a Badge and reuses it, impersonating an authorized device, when a device in unauthenticated domain requests for an authentication.

Prevention: The transmission of a Badge is always encrypted with receiver's public key. This makes it hard for an adversary to get a Badge itself without possessing receiver's private key. However, we can think that the adversary intercepts the message encrypted with receiver's public key which includes a Badge. The adversary then reuses it appropriately when authentication is requested by a device in unauthenticated domain. In this case, the receiver figures out that the device's identity does not match with the identity in the Badge when it opens the Badge.

V. Conclusions

In this paper, we have proposed a reliable and adaptable authentication and secure channel establishment protocol for multi-hop wireless home environment. Central to our design effort is the authentication by a neighboring device, on behalf of the server, in a multi-hop wireless home networks, while supporting mutual authentication and minimizing reliance on public key cryptographic operation. In addition to this, our protocol supports efficient and flexible channel establishment among heterogeneous devices after authentication. Through security analysis, we show our protocol is secure because it is resistant to various attacks. Further, it is efficient and adaptable for multihop wireless home network because it minimizes overheads such as communication and computation costs.

Acknowledgement

This work is supported in part by a grant from the Center for Embedded Systems (CES).

References

[1] *Zigbee Specification*, version 1.0, http://www.zigbee.org.
[2] S. Lee, S. Banerjee, and B. Bhattacharjee, *The Case for a Multihop Wireless Local Area Network*, Proc. IEEE INFOCOM, vol. 2, pp: 941-951, Mar. 2004.
[3] *Bluetooth Specification*, http://www.bluetooth.com.
[4] Multi-hop Mesh Network, http://www.intel.com/technology/comms/cn02032.htm.
[5] P. Krishnamurthy, J Kabara, and T. Anusas-amornkul, *Security in Wireless Residential Network*, IEEE Transactions on Consumer Electronics, Feb 2002.
[6] T.D. Taman et al., *Algorithm-agile encryption in ATM networks*, IEEE Computer, pp. 57-64, Sep 1998.