Scientific Journal Impact Factor (SJIF): 1.711

e-ISSN: 2349-9745
p-ISSN: 2393-8161

International Journal of Modern Trends in Engineering and Research
www.ijmter.com

SURVEY OF TRUST BASED BLUETOOTH AUTHENTICATION FOR MOBILE DEVICE

P.Sindhuja[1], S.Uma[2], D.Deepachandra[3], M.Poovizhi[3]
[1,2,3,4]Computer Science and Engineering, Hindustan Institute of Technology

Abstract- Practical requirements for securely demonstrating identities between two handheld devices are an important concern. The adversary can inject a Man-In- The-Middle (MITM) attack to intrude the protocol. Protocols that employ secret keys require the devices to share private information in advance, in which it is not feasible in the above scenario. Apart from insecurely typing passwords into handheld devices or comparing long hexadecimal keys displayed on the devices' screen, many other human-verifiable protocols have been proposed in the literature to solve the problem. Unfortunately, most of these schemes are unsalable to more users. Even when there are only three entities attempt to agree a session key, these protocols need to be rerun for three times. So, in the existing method a bipartite and a tripartite authentication protocol is presented using a temporary confidential channel. Besides, further extend the system into a transitive authentication protocol that allows multiple handheld devices to establish a conference key securely and efficiently. But this method detects only the outsider attacks. Method does not consider the insider attacks. So, in the proposed method trust score based method is introduced which computes the trust values for the nodes and provide the security. The trust score is computed has a positive influence on the confidence with which an entity conducts transactions with that node. Network the behavior of the node will be monitored periodically and its trust value is also updated .So depending on the behavior of the node in the network trust relation will be established between two nodes.

Keywords- Bluetooth, Authentication, Seeing-is- Believing (SiB), Quick Response Code, Discrete logarithm problem.

I. INTRODUCTION

1.1 ANDROID

Android is a mobile operating system developed by Google. It is used by several smart phones, such as the Motorola Droid, the Samsung Galaxy, and Google's own Nexus One. The Android operating system (OS) is based on the open Linux kernel. Unlike the phone OS, Android is open source, meaning developers can modify and customize the OS for each phone. Therefore, different Android-based phones may have different graphical user interfaces GUIs even though they use the same OS.

Android phones typically come with several built-in applications and also support third-party programs. Developers can create programs for Android using the free Android SDK (Software Developer Kit). Android programs are written in Java and run through Google's "Davlik" virtual machine, which is optimized for mobile devices. Users can download Android "apps" from the online Android Market. Since several manufacturers make Android-based phones, it is not always easy to tell if a phone is running the Android operating system. If you are unsure what operating system a phone uses, you can often find the system information by selecting g "About" in the Settings menu. The name "Android" comes from the term android, which refers to a robot designed to look and act like a human.

II. LITERATURE SURVEY

Two entities, who only share a password, and who are communicating over an insecure network, want to authenticate each other and agree on a large session key to be used for protecting their subsequent communication. This is called the password-authenticated key exchange problem. If one of the entities is a user and the other is a server, then this can be seen as a problem in the area of remote user access. Many solutions for remote user access rely on cryptographically secure keys, and consequently have to deal with issues like key management, public-key infrastructure, or secure hardware. Many solutions that are password-based, like telnet or Kerberos, have problems that range from being totally insecure (telnet sends passwords in the clear) to being susceptible to certain types of attacks (Kerberos is vulnerable to o®-line dictionary attacks.

A new password-authenticated key exchange protocol called PAK (Password Authenticated Key exchange) is presented which provides perfect forward secrecy and is proven to be as secure as Decision Diffie-Hellman in the random oracle model. Compared to the protocol of, PAK (1) does not require the RSA assumption, (2) has fewer rounds, and (3) is conceptually simpler, with a simpler proof. Compared to the protocol, PAK does not require an ideal block cipher assumption for security, but has a more complicated proof.

In the full work, also show how the security of PAK can be related to the Computational Diffie-Hellman problem. In addition to PAK, also show a more efficient 2 round protocol called PPK (Password-Protected Key exchange) that is provably secure in the implicit- authentication model. Then extend PAK to a protocol called PAK-X, in which one side (the client) stores a plaintext version of the password, while the other side (the server) only stores a verifier for the password. Formally prove security of PAK-X, even when the server is compromised. Security in this case refers to an attacker not being able to pose as a client after compromising the server; naturally, it would be trivial to pose as the server. Limitations are consider as high complexity and highly expensive. Entity authentication and authenticated key establishment are of fundamental importance in establishing secure communications between a pair of communicating parties.
Entity authentication is normally provided when a communications link is established and, if an authenticated key is established simultaneously, this can be used to protect subsequently exchanged data. The purpose of this work is to examine how these services might best be achieved for personal wireless-enabled devices. Manual authentication techniques have been designed to enable wireless devices to authenticate one another via an insecure wireless channel with the aid of a manual transfer of data between the devices. Manual transfer refers to the human operator of the devices performing one of the following procedures: copying data output from one device into the other device, comparing the output of the two devices, or entering the same data into both devices.

Techniques currently being standardized are described which achieve this, and which require only small amounts of data to be transferred between the two devices. This makes the mechanisms particularly attractive for non-expert use, as required for ubiquitous mobile wireless devices. Limitations are consider as High storage is required and less secure. Security in wireless network is becoming more and more important while the using of mobile equipment’s such as cellular phones or laptops is tremendously increasing. Due to the unique characteristic of wireless network, unlike wire line networks, to achieve this goal is never a trivial challenge. Mobile ad hoc networks (MANETs) is a special wireless network which does not rely on any fixed infrastructure but depends on the cooperation between each node like a cellular phone in the network. In this essay discuss the possible attacks in MANETs and briefly discuss the solutions aimed to these problems.

Address the problem of secure communication and authentication in ad-hoc wireless networks. This is a difficult problem, as it involves bootstrapping trust between strangers. A user-friendly solution is presented which provides secure authentication using almost any established public-key-based key exchange protocol, as well as inexpensive hash-based alternatives. In this approach, devices exchange a limited amount of public information over a privileged side channel, which will then allow them to complete an authenticated key exchange protocol over the wireless link. This solution does not require a public key infrastructure, is secure against passive attacks on the privileged side channel and all attacks on the wireless link, and directly captures users' intuitions that they want to talk to a particular previously unknown device in their physical proximity limitations are consider as High complexity and Communication cost is high.

Obtaining authenticated values from devices in ways that are easily understandable by non-expert users is currently an open problem. The Seeing-Is-Believing is analyzed which is a system that utilizes 2D barcodes and camera phones to implement a visual channel for authentication and demonstrative identification of devices. As camera-equipped mobile phones rapidly approach ubiquity, these devices become a naturally convenient platform for security applications that can be deployed quickly and easily to millions of users. Today's mobile phones increasingly feature Internet access and come equipped with cameras, high-quality displays, and short range Bluetooth wireless radios.

They are powerful enough to perform secure public key cryptographic operations in fewer than one second. Propose to use the camera on a mobile phone as a new visual channel to achieve demonstrative identification of communicating devices formerly unattainable in an intuitive way. This approach is termed as Seeing-Is-Believing (SiB). In SiB, one device uses its camera to take a snapshot of a barcode encoding cryptographic material identifying, e.g., the public key of another device. This is called as a visual channel. Barcodes can be pre-configured and printed on labels attached to devices, or they can be generated on-demand and shown on a device's display.

Apply this visual channel to several problems in computer security. SiB can be used to bootstrap authenticated key exchange between devices that share no prior context, including such devices as mobile phones, wireless access points, and public printers. The SiB is used to aid in the establishment of a trusted path for configuration of a TCG-compliant1 computing platform, and to provide the user with assurance in the integrity of an application running on a TCG-compliant computing platform. Also use SiB to secure device configuration in the context of a smart home. Limitations are consider as Unaware of any attacks feasible today which result in anything but noise from the camera under attack.

III. EXISTING WORK

Practical requirements for securely demonstrating identities between two handheld devices are often omitted by theoretical protocol designers. Existing system, a scheme is developed named Seeing-is-Believing (SiB) which uses the display of a mobile phone to demonstrate its identity to a handheld device equipped with a screen.

The idea of their scheme is that a handheld device generates a temporal public key and sends it to another handheld device through the wireless channel, like Bluetooth. This device also creates a commitment of the public key in the form of a visual code, and displays the code as a digital image on its display. The other handheld device photographs this code using its screen and verifies the public key using this public key commitment. This public key allows the receiver to authenticate the sender after executing some simple confirmation steps. Yet, there are also some disadvantages in Sib the first problem is scalability. Sib protocol supports secure authentication for two handheld devices. Adopting transitive authentication may solve the scalability problem. If the devices owners trust each other in the way that each participant would not intentionally eavesdrop other parties' communication and damage the protocol, it is possible to simplify the protocol. The idea of transitive authentication says that a device can authenticate other strange devices through another broker.

Solve the second problem, attempt to propose a method that only requires one photo-taking. To observe that most mobile phones and PDAs have their cameras located at the back of the devices. When the devices are taking photo of each other screens, it is very likely that a device's monitor will be covered by another device. It means that the visual code displayed on the device cannot be easily obtained by hidden adversary.

The adversary may utilize a highly sophisticated telescope to capture the screen of the user's device. Fortunately, this can be prevented with a privacy protection filter on the mobile device's display. As a result, it is reasonable to believe that short range photo taking provides not only data integrity but also data confidentiality. In that case, it is possible for us to devise a system that takes only one photo during the authentication protocol.

3.1.1 Limitations of the Existing System

The Existing System has the limitations which are related to the knowledge about the different attributes and the other is about the algorithm used in existing system and the last is that which deals with the performance of the system. Some of the Limitations of the existing system are given below;

- Insider attack is not detected
- Less efficient
- Less security.

IV. PROPOSED WORK

Trust score based method is introduced which computes the trust values for the nodes and provide the security. Trust is an important aspect of mobile devices. It enables entities to cope with uncertainty and uncontrollability caused by the free will of others. Trust computations and management are highly challenging issues in mobile devices due to computational complexity constraints, and the independent movement of component nodes. This prevents the direct application of techniques suited for other networks.

QR code (abbreviated from Quick Response Code). The QR Code system has become popular outside the automotive industry due to its fast readability and greater storage capacity compared to standard UPC barcodes. Applications include product tracking, item identification, time tracking, document management, general marketing. A QR code consists of black modules (square dots) arranged in a square grid on a white background, which can be read by an imaging device (such as a camera) and processed using Reed–Solomon error correction until the image can be appropriately interpreted. The required data are then extracted from patterns present in both horizontal and vertical components of the image.

Reputation based Trust Score Calculation for mobile devices have been proposed. This architecture is for establishment of the trust for a newly entering node in the mobile devices. Method the behavior of the node will be monitored periodically and its trust value is also updated .So depending on the behavior of the node in the network trust relation will be established between two nodes.

4.1 MODULE DESCRIPTION

- Pairing of Bluetooth devices Module
- Initialization process Module
- Bipartite Authentication Protocol Module
- Tripartite Authentication Protocol Module

1.1.1 Pairing of Bluetooth devices Module

The two devices are connected to transmit the data. Firstly, Request the BLUETOOTH PERMISSION in order to perform any Bluetooth communication, such as requesting a connection, accepting a connection and transferring the data. After that, Device discovery is a scanning procedure and searches the local area for Bluetooth enabled devices. If the Bluetooth device is currently enabled to be discoverable then only it will respond to the discovery request. If the device is discoverable then it will respond by sharing some information such as device name, class and its unique MAC address. First time connection request automatically presented to the user. The information can be read using the Bluetooth APIs.

4.1.2 Pairing of Bluetooth devices Module

The two devices are connected to transmit the data. Firstly, Request the BLUETOOTH PERMISSION in order to perform any Bluetooth communication, such as requesting a connection, accepting a connection and transferring the data. After that, Device discovery is a scanning procedure and searches the local area for Bluetooth enabled devices.

If the Bluetooth device is currently enabled to be discoverable then only it will respond to the discovery request. If the device is discoverable then it will respond by sharing some information such as device name, class and its unique MAC address. First time connection request automatically presented to the user. The information can be read using the Bluetooth APIs.

4.1.3 Initialization process Module

Bilinear pairing is a main component in constructing our tripartite protocol. Firstly briefly review some basic facts of bilinear pairing. Let G_1 be an additive group with order q and G_2 be a multiplicative group. Given P is a generator of G_1 assume discrete logarithm problem (DLP) is hard in G_1 i.e., given the instance p, aP it is difficult to calculate a. To say a mapping function e is bilinear if $e: G_1 \times G_1 \rightarrow G_2$ satisfies the following properties:

Bilinearity: $e(aP, bQ) = e(P, Q)^{ab}$ for all $P, Q \in G_1$ and$a, b \in Z_p^*$. Also for $P, Q, R \in G_1, e(P + Q, R) = e(P, R)e(Q, R)$ and $e(P + Q, R) = e(P, Q)e(P, R)$.

Non-degeneracy: $e(P, P)$ is the generator of G_2 if P is the generator ofG_1. In other words, $e(P, P) \neq 1$.

Computable: There exist an efficient algorithm to compute $e(P, Q)$.

Next, state some famous hard problems related to bilinear pairings and elliptic curves.

Computational Diffie-Hellman Problem (CDH): The CDH problem states that given two elements $A = aP, B = bP$ and a generator P in G_1 as inputs where $a, b \in Z_p^*$ output abP. An algorithm $\mathcal{A}$ has advantage ϵ in solving CDH if

$$\Pr\{\mathcal{A}(aP, bP, P) = abP\} \geq \epsilon$$

Where the probability is over the random choice of generator $P \in G_1$ the random choice of $a, b \in Z_p^*$ and the random bits consumed by$\mathcal{A}$.CDH assumption: To say that the $(t, \epsilon) - CDH$ assumption holds in G_1 if no t-time algorithm has an advantage more than ϵin solving CDH problem inG_1.Bilinear Diffie-Hellman Problem (BDH): The BDH problem states that given three elements$A = aP, B = bP, C = cP$, a generator P in G_1 and a bilinear pairing function $e: G_1 \times G_1 \to G_2$ as inputs, where $a, b, c \in Z_p^*$ output$e(P, P)^{abc}$. An algorithm $\mathcal{A}$ has advantage ϵ in solving BDH if

$$Pr(\mathcal{A}(aP, bP, cP, P, e) = e(P, P)^{abc}\} \geq \epsilon$$

Where the probability is over the random choice of generator $P \in G_1$ the random choice of $a, b, c \in Z_p^*$ and the random bits consumed by$\mathcal{A}$.
BDH assumption: To say that the $(t, \epsilon) - BDH$ holds in G_1 to G_2 if no $t - time$ algorithm has an advantage more than ϵ in solving BDH problem using bilinear map$e: G_1 \times G_1 \to G_2$.

4.1.4 Bipartite Authentication Protocol Module

Present the bipartite authentication protocol using encryptions E and MACs M. Assume there are two handheld devices A and B want to authenticate each other such that A is equipped with a high resolution display and B is equipped with a camera. A initiates the protocol by randomly selecting an integer $a \in Z_p^*$ calculating $Pa = aP$ and generating two k-bits long random keys K_{a_1} andK_{a_2}. Then, A calculates and sends the following tuples to B.

$$(C_{1.1}, C_{1.2}, C_{1.3}) = (E_{K_{a_1}}(P_a)M_{K_{a_2}}(C_{1.1}||A), A)$$

At the same time, it encodes K_{a_1} andK_{a_2} into a visual code and displays it on screen. Note that P_a is encrypted; thus, the adversary cannot forge valid MAC value and further launch MITM attack.

After receiving the tuples above, B takes a photograph of the visual code with its screen to obtain the key $\widehat{K}_{a_1}$ and$\widehat{K}_{a_2}$. Then, it verifies the tuples using $\widehat{K}_{a_2}$ and decrypts $C_{1.1}$using $\widehat{K}_{a_1}$ to obtain$\widehat{P}_a$. If the message is authenticated, B will consider A is a trusted device. Otherwise, it will terminate the process.

B also selects a random integer $b \in Z_p^*$ and calculates $P_b = bP$. After that, it computes$K_{ab} = H_1(b.\widehat{P}_a)$. Finally, it prepares the following tuples and sends them to A.

$$(C_{2.1}, C_{2.2}, C_{2.3}) = M_{K_{ab}}(A||B), P_b, B)$$

After receiving the tuples from B,A computes $\widehat{K}_{ab} = H_1(a.C_{2.2})$. Then, A verifies if $C_{2.1} = M_{\widehat{K}_{ab}}(A||B)$. If it does, A will authenticate B as a trusted device. Each of them will utilize a l-bit key $K = H_2(a.\widehat{P}_b) = H_2(b.\widehat{P}_a)$ as their session key for further communication. The completeness of the protocol is asserted by assuming there is no adversary in the environment. Notice that$K_{ab} = H_1(b.\widehat{P}_a) = H_1(a.\widehat{P}_b)$. Therefore A and B will be mutually authenticated if the tuples they send are unaltered.

4.2 Advantages of the Proposed System

- Insider attack is detected
- High efficient
- High secure

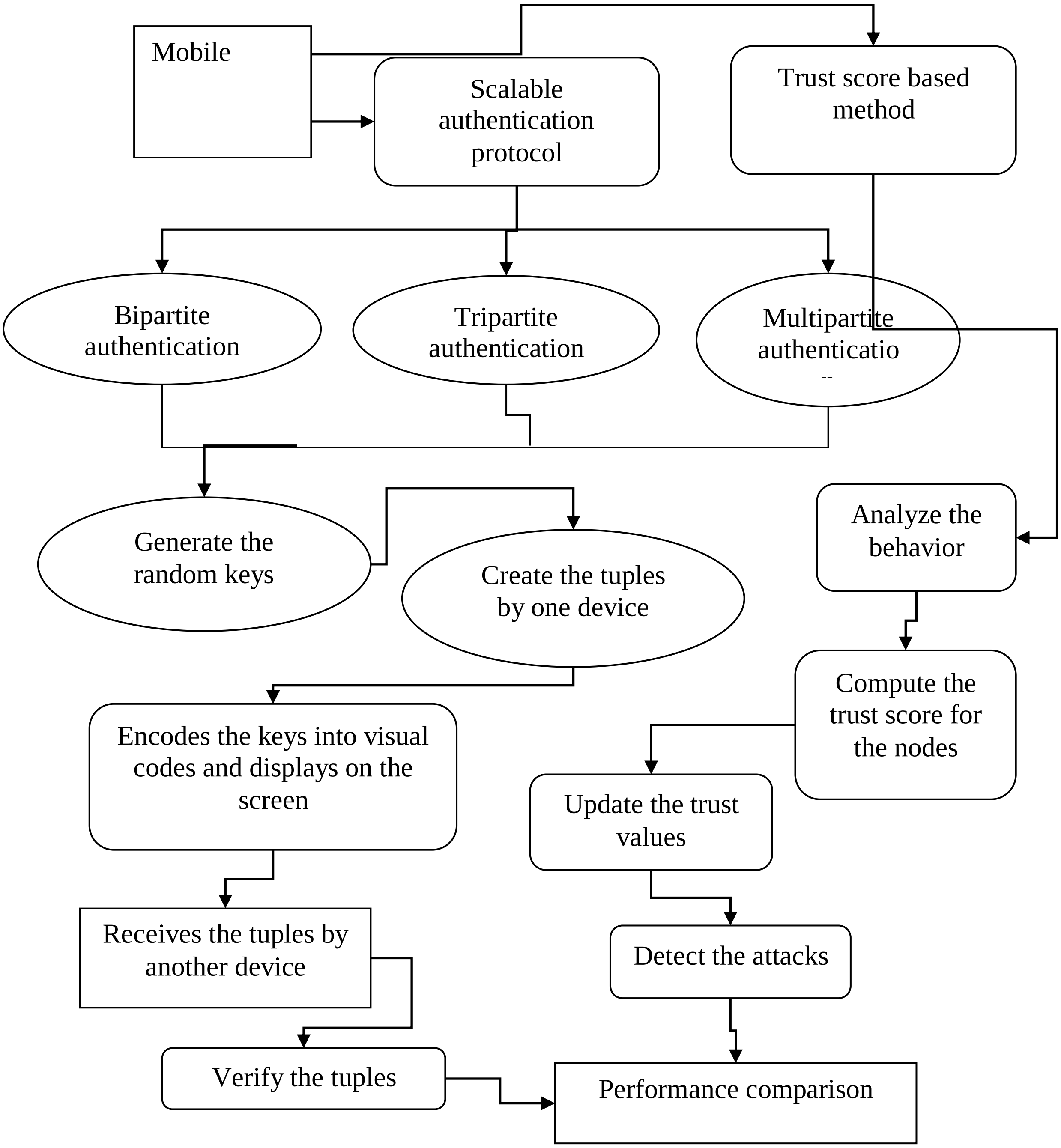
Mobile
Scalable authentication protocol
Trust score based method
Bipartite authentication
Tripartite authentication
Multipartite authenticatio
Generate the random keys
Create the tuples by one device
Analyze the behavior
Compute the trust score for the nodes
Encodes the keys into visual codes and displays on the screen
Update the trust values
Receives the tuples by another device
Detect the attacks
Verify the tuples
Performance comparison

Fig 2.1 System Architecture Diagram

V. CONCLUSION

Agreeing key in ad-hoc environment securely is an important topic. Most of the previous schemes only focus on two parties' case and are overcomplicated. In this work the efficient key agreement protocols are developed for two and three handheld devices over temporal confidential and authenticated channels.

They simplify previous unnecessary complications and reduce the bottleneck of running time – human's involvements. This system enjoys several nice properties including efficient, human error proof, and secure. By satisfying the above practical requirements, these protocols have improved previous scheme significantly. But the insider attacks are not detected in this method.

REFERENCES

[1] Apkun S.C, Hubaux .J, and Buttya´n .C, "Mobility helps security in ad hoc networks," in Proc. of the 4th ACM Symposium on Mobile ad hoc Networking & Computing, 2011, pp. 46–56.

[2] Barua .R, Dutta .R, and Sarkar .P, "Extending Joux's protocol to multi party key agreement," in Progress in Cryptology–INDOCRYPT, 2003, pp. 205–217.

[3] Balfanz .D, Smetters .D, Stewart .P, and Wong .H, "Talking to strangers: Authentication in ad-hoc wireless networks," in Proc. of the 9th Symposium on Network and Distributed System Security Symposium

[4] Blake-Wilson .S and Menezes .A,"Entity authentication and authenticated key transport protocols employing asymmetric techniques," Security Protocols Workshop, vol. 97, 1997.

[5] Bellare .M and Rogaway .P, "Entity authentication and key distribution," in Proc. of the Advances in Cryptology-CRYPTO, vol. 773, 1993, pp. 232–249.

[6] Boyko .V, MacKenzie .P, and Patel .S, "Provably Secure Password- Authenticated Key Exchange Using Diffie-Heilman," Proceedings of the Advances in Cryptology-Eurocrypt, 2009

[7] Bellovin S.M, and Merritt.M, "Augmented encrypted key exchange: a password-based protocol secure against dictionary attacks and password file compromise," in Proc. 1st ACM conf. on Computer and Communications Security, pp. 244–250.

[8] Gehrmann .C, Mitchell .C, and Nyberg .K, "Manual authentication for wireless devices," RSA Cryptobytes, vol. 7, no. 1, pp. 29–37, 2004

[9] Bluetooth .S, "The official Bluetooth wireless info site," 2011.

[10] Chen et al., "GAnGS: Gather, authenticate 'n group securely," in Proc. of the 4th ACM Inter. Conf. on Mobile Computing and Networking. ACM New York, NY, USA, pp. 92–103.