© 2016 IJSRSET | Volume 2 | Issue 3 | Print ISSN : 2395-1990 | Online ISSN : 2394-4099
Themed Section: Engineering and Technology

Thwarting Attackers in the Wireless Networks without Trusted Authorities

P. Ganesh, M. Praba
Department of Computer Science and Engineering, Surya School of Engineering and Technology, Tamilnadu, India

ABSTRACT

Due to the broadcast nature of the wireless medium, wireless networks are especially vulnerable to Sybil attacks, where a malicious node illegitimately claims a large number of identities and thus depletes system resources. A wireless sensor network consists of many sensor nodes which are deployed to monitor physical or environmental conditions and to pass the collected data to a base station. Though wireless sensor network is subjected to have major applications in all the areas, it also has many security threats and attacks. Among all threats such as sinkhole, wormhole, selective forwarding, denial of service and node replication, Sybil attack is a major attack where a single node has multiple identities. When a Sybil node acts as a sender, it can send false data to its neighbors. When it acts as receiver, it can receive the data which is originally destined for a legitimate node. Further, we note that prior signal print methods are easily defeated by mobile attackers and develop an appropriate challenge-response defense. Finally, we present the Mason test, the first implementation of these techniques for ad hoc and delay-tolerant networks. A message can be sent to the receiver directly without trusted authorities.

Keywords: Wireless Networks, Signal Print, Security, Sybil Attack.

I. INTRODUCTION

The open nature of wireless ad hoc networks (including delay-tolerant networks [1]) enables applications ranging from collaborative environmental sensing [2] to emergency communication [3], but introduces numerous security concerns since participants are not vetted. Solutions generally rely on a majority of the participants following a particular protocol, an assumption that often holds because physical nodes are expensive. However, this assumption is easily broken by a Sybil attack. A single physical entity can pretend to be multiple participants, gaining unfair influence at low cost [4]. Newsome et al. survey Sybil attacks against various protocols [5], illustrating the need for a practical defense. Proposed defenses fall into two categories. Trusted certification methods [7], [8] use a central authority to vet potential participants and thus are not useful in open ad hoc (and delay- tolerant) networks. Resource testing methods [9], [10], [11], [12] verify the resources (e.g., computing capability, storage capacity, real-world social relationships, etc.) of each physical entity. Most are easily defeated in ad hoc networks of resource-limited mobile devices by attackers with access to greater resources, e.g., workstations or data centers. One useful class of defenses is based on the natural spatial variation in the wireless propagation channel, an implicit resource. Channel responses are uncorrelated over distances greater than half the transmission wave-length [13] so two transmissions with the same channel response are very likely to be from the same location and device [14], [15]. Note that two transmitters may be close enough; One class of Sybil defenses based on this observation uses specialized hardware to accurately measure and compare channel responses [15]. However commodity devices are not equipped with such hardware. Commodity devices expose an aggregate, scalar value, the received signal strength points. In open ad hoc networks, observations are untrusted, coming from potentially lying neighbors. In this case observations falsified by attackers can lead to incorrect conclusions. Trust-less methods have been proposed, but have various limitations (e.g., devices must have uniform transmit power [20] or the method may be used only in outdoor environments with predictable propagation ranges [21]). Instead, a general method to separate true and false observations is needed. Traditionally, secure communication is achieved by using cryptographic technologies such as encryption with a key concept.

II. METHODS AND MATERIAL

1. Related Works

The existing mechanisms include centralized and decentralized approaches. The vast implemented solution is trusted certification [12], [13]. This solution assumes that there is a special trusted third party or central authority, which can verify the validity of each participant, and further issues a certification for the honest one. In reality, such certification can be a special hardware device or a digital number. Note that essentially both of them are a series of digits, but are stored on different media. Before a participant joins a peer-to-peer system, provides votes, or obtains services from the system, first his identity must be verified. This method gets its limitation when it is applied for larger network. Another method works based on the resource used by the node. If a Sybil node exists then it has to perform the tasks of the identities it possess. So when it exceeds a threshold value then the Sybil node is detected. [14].Secret key [15] can also be shared but it consumes more power as it involves in complex encryption and decryption techniques. In contrast to existing solutions that are based on sharing encryption keys, RSSI based scheme [16] presents a solution for Sybil attack based on received signal strength indicator (RSSI) readings of messages. Though it is said to be lightweight (i.e., only one message communication), it is time-varying, unreliable and radio transmission is non-isotropic.

2. Problem Formulations and Background

In this section, we define our problem, summarize the solution framework, describe our attack model, and briefly review the signal print method.

2.1 Problem Formulation

Our goal is to extend signal print-based Sybil detection methods to work without a priori trust in any observer, allowing any participant in an open wireless network to determine which of its one-hop neighbor's is non-Sybil. In the wireless network, specifically data can be indirectly with an intermediate nodes or trusted authorities. So the intermediate nodes or trusted authorities may acts as an attacker. We formulate the system without an intermediate nodes or trusted authorities. The user has proper authentication to access the data. Authorized user should be provided with an encrypted file and a key to access their files. Finally, admin views all the user and attackers activities and send the data to the authenticated user.

2.2 Attack Model

We model attackers who operate commodity devices, but not specialized hardware. Commodity devices can be obtained in large scale by compromising those owned by normal network participants, a more practical attack vector than distributing specialized hardware at the same scale. Specifically, we assume attackers have the following capabilities and restrictions.

1) Attackers may collude through arbitrary side channels.
2) Attackers may accumulate information, e.g., RSSIs, across multiple rounds of the Mason test.
3) Attackers have limited ability to predict the RSSI observations of other nodes.
4) Attackers can control transmit power for each packet, but not precisely or quickly steer the output in a desired direction, i.e., they are not equipped for antenna array-based beam-forming.
5) Attackers can move their devices, but cannot quickly and precisely switch them between multiple positions, e.g., they do not have high-speed, automated electromechanical control.

One common denial-of-service (DOS) attack in wireless networks jamming the channel cannot be defended against by commodity devices. Thus, we do not defend against other more-complicated DOS attacks. However, note that ad hoc and delay-tolerant networks are much more resistant than infrastructure networks to such attacks, because a single attack can affect only a small portion of the network.

Moreover, DOS attacks are less catastrophic to privacy and security than successful Sybil attacks. Notably, we assume attackers do not have per- antenna control of MIMO (Multiple-Input and Multiple- Output) [23] devices. Such control would defeat the signal print method (even with trusted observers), but is costly to implement. Commodity MIMO devices do not expose this control to software and thus are not suitable attack vectors. Distributing specialized MIMO-capable hardware over large portions of the network would be prohibitively expensive. We believe that the signal print method can be extended to MIMO systems. Our focus is extending signal print-based methods to ad hoc networks of commodity devices by removing the requirement for trusted observations.

2.3 The Mason Test

This section describes the full Mason test protocol, an implementation of the concepts introduced in the previous sections. There are four main requirements on the protocol.

1) Conforming neighbors must be able to participate. That is, selective jamming of conforming identities must be detectable.

2) Probe packets must be transmitted in pseudo- random order. Further, each participant must be able to verify that no group of identities controlled the order

3) Moving identities must be rejected. To save energy and time, conforming nodes that are moving when the protocol begins should not participate.

We assume a known upper bound on the number of conforming neighbors, i.e., those within the one-hop transmission range. In most applications, a bound in the hundreds (we use 400 in our experiments) will be acceptable. If more identities attempt to participate, the protocol aborts and no classification is made. This appears to open a denial-of-service attack. However, we do not attempt to prevent, instead only detect, DOS attacks, because one such attack simply jamming the wireless channel is unpreventable (with commodity hardware).

3. Geometrical Analysis of Sybil Attacks

In this section, we provide a geometrical characterization of the success area of a Sybil attack. We begin with some notations and the problem formalization.

Let us consider S and R be two mobile nodes such that S sends some messages received by R. We assume that the transmission of a single message is immediate, allowing to consider the positions of S and R as fixed points of the space at the time of transmission. We denote by d(S,R) the distance between S and R. Let denote by Psnd the sending power of the node S. With an isotropic antenna of gain Gsnd and for d(S,R) sufficiently large, the node R will receive a power Prcv equals to:

Prcv = Psnd × Gsnd ×Grcv × λ^2 $16\pi^2$ ×d2(S,R) , where λ denotes the wavelength of the radiation.

By denoting GSR = Gsnd×Grcv×λ2/(16π2) the gain of the link from S to R, the maximal power Pmax rcv (dist(S,R)) at distance d(S,R) from the sender can be rewritten as:

Pmax rcv (d(S,R)) = Psnd ×GSR × d2(S,R) (1)

By taking into account signal attenuation, the power received by R is smaller than Pmax rcv :

Prcv(d(S,R)) = α×Pmax rcv (d(S,R)) 0≤α≤1 (2)

Where α depends on several parameters (distance d(S,R), λ, atmospheric conditions...). We denote by dmin the minimal distance between the antenna of a sender and the antenna of a receiver. We can define the maximal received power Pmax rcv for a receiver close to a sender as:

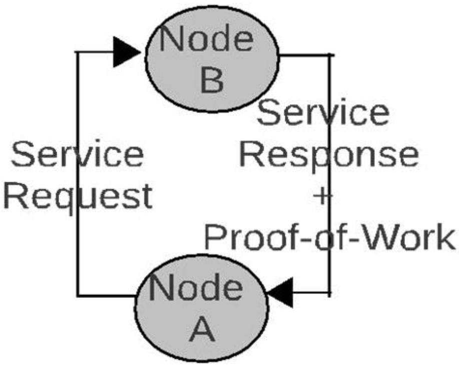
Pmax rcv = Psnd ×GSR × 1 d2min (3)

4. Overview

The goal of Sybil Control (or other Sybil prevention schemes) is not to completely prevent adversaries from joining the system, but rather to place a limit on the number of additional Sybil nodes adversaries can join, thereby preventing them from obtaining significant influence over the system. Sybil Control operates towards this goal using the following insight: if a computational cost is incurred by nodes before they are allowed to join the system, then adversaries with finite resources will have an upper bound on the rate they can acquire identities.

Moreover, if nodes are required to periodically repay this computational cost to retain their identifiers, then the number of identifiers that can be maintained by the adversary will be limited. To leverage this insight, Sybil Control controls admission and retainment of nodes into a system. To do this, Sybil Control provides a distributed enforcement mechanism to allow network participants to collectively verify that their neighbors are paying computational costs (through the use of puzzles) to remain in the system. In particular, Sybil Control provides mechanisms to address two key challenges:

Moreover, if nodes are required to periodically repay this computational cost to retain their identifiers, then the number of identifiers that can be maintained by the adversary will be limited. To leverage this insight, Sybil Control controls admission and retainment of nodes into a system. To do this, Sybil Control provides a distributed enforcement mechanism to allow network participants to collectively verify that their neighbors are paying computational costs (through the use of puzzles) to remain in the system. In particular, Sybil Control provides mechanisms to address two key challenges:



A. Collectively verifying a node

In a distributed system, we lack a centralized authority to verify puzzle solutions of new arrivals. To address this, Sybil- Control allows decentralized groups of nodes to collectively verify the computational work done by their neighbors. For example, before a node A trusts communication with another node B, A requires B to prove that it recently solved a puzzle. If B is a malicious Sybil node and chooses not to solve the puzzles, it will not be able to provide proof-of-work.

Defense mechanisms in Sybil Control protect honest nodes like A from using B, essentially making B non-functional in the system and preventing it from doing harm. This forces adversaries to use only puzzle-solving Sybil's, of which they can support a limited number. To establish recurring proof-of-work, Sybil Control uses a distributed collective verification scheme, where nodes periodically challenge each other to solve new puzzles. Following this scheme, if a group of nodes B1, B2, and B3 collectively desire to communicate with another node A, they each periodically create, record, and send new challenges to A. A also periodically creates a new challenge using the latest received challenges, and uses that new challenge to solve a new puzzle. When any one of the nodes requests a service from A, for example nodes B1, A responds with the service as well as information from the latest puzzle it solved. If B1 still has recorded the original challenge used in the puzzle, B1 can verify A's puzzle solution. The duration for which B1 records challenges can put a bound on how recent A's solution is, validating its timeliness. If all nodes in the network formed a single group and collectively challenged each other, then all pairs of nodes can perform direct verification.

B. Verifying across multiple hops

Performing direct verification between all pairs of nodes in the network can be prohibitively expensive. While it may scale to systems that communicate in a full mesh (e.g., one- hop overlay networks), many systems restrict the number of neighbors a node is allowed to communicate with for scaling purposes (e.g., in DHTs like Chord, nodes maintain regular communication relationships with only a logarithmic number of adjacent neighbors). To support these systems, Sybil Control provides a multi-hop verification scheme.

To do this, nodes in Sybil Control only exchange challenges with their neighbors. Neighbor relationships may be selected arbitrarily, or in a manner based on the instrumented distributed system (e.g., when applying Sybil Control to the Chord DHT, challenges may be exchanged only with a node's fingers and successors). Each node, then performs a cryptographic aggregation step to combine the challenges received by its neighbors, and uses this aggregation as input to construct its own challenges to be sent to its neighbors. This process repeats, allowing a node's challenge to be distributed throughout the network. Sybil Control provides a multi-hop verification mechanism, allowing a node to check whether its challenge is indirectly incorporated by a remote node. This allows indirect proof-of-work to be established between a node and non-neighbors.

III. CONCLUSION

We have described a method to use signal prints to detect Sybil attacks in open ad hoc and delay-tolerant networks without requiring trust in any other node or authority. We use the inherent difficulty of predicting RSSIs to separate true and false RSSI observations reported by one-hop neighbors. Attackers using motion to defeat the signal print technique are detected by requiring low- latency retransmissions from the same position.

The Mason test was implemented on HTC Magic smart phones and tested with human participants in three environments. It eliminates 99.6%–100% of Sybil identities in office environments, 91% in a crowded high- motion cafeteria, and 96% in a high-motion open outdoor environment. It accepts 88%–97% of conforming identities in the office environments, 87% in the cafeteria, and 61% in the outdoor environment. The vast majority of rejected conforming identities were eliminated due to motion. Without intermediate nodes or trusted authorities, data can be sent to the original users. And the unknown users or attackers can be found by this way data can be transferred securely in the network.

IV. REFERENCES

[1] P. Hui, J. Crowcroft, and E. Yoneki, "BUBBLE rap: Social-based for- warding in delay tolerant networks," IEEE Trans. Mobile Computing, vol. 10, no. 11, pp. 1576–1589, Nov. 2011.

[2] Y. Xiang, L. S. Bai, R. Piedrahita, R. P. Dick, Q. Lv, M. P. Hannigan, and L. Shang, "Collaborative calibration and sensor placement for mobile sensor networks," in Proc. Int. Conf. Information Processing in Sensor Networks, Apr. 2012, pp. 73–84.

[3] P. Gardner-Stephen, "The Serval project: Practical wireless ad-hoc mobile telecommunications," Flinders University, Adelaide, South Australia, Tech. Rep., Aug. 2011.

[4] J. Douceur, "The Sybil attack," in Proc. Int. Wkshp. Peer-to-Peer Systems, Mar. 2002, pp. 251–260.

[5] J. Newsome, E. Shi, D. Song, and A. Perrig, "The Sybil attack in sensor networks: Analysis & defenses," in Proc. Int. Conf. Information Processing in Sensor Networks, Apr. 2004, pp. 259–268.

[6] B. N.Levine, C. Shields, and N. B. Margolin, "A survey of solutions to the Sybil attack," Department of Computer Science, University of Massachusetts Amherst, Amherst, MA, Tech. Rep., Oct. 2006.

[7] H. Zhou, M. Mutka, and L. Ni, "Multiple-key cryptography-based distributed certification authority in mobile ad-hoc networks," in Proc. Global Telecommunications Conf., Nov. 2005.

[8] M. Ramkumar and N. Memon, "An efficient key pre distribution scheme for ad hoc network security," IEEE J. Selected Areas in Communications, vol. 23, pp. 611–621, Mar. 2005.

[9] N. Borisov, "Computational puzzles as Sybil defenses," in Proc. Int. Conf. Peer-to-Peer Computing, Sept. 2006, pp. 171–176.

[10] F. Li, P. Mittal, M. Caesar, and N. Borisov, "Sybil Control: Practical Sybil defense with computational puzzles," in Proc. Wkshp. Scalable Trusted Computing, Oct. 2012.

[11] H. Yu, M. Kaminski, P. B. Gibbons, and A. Flaxman, "Sybil Guard: defending against Sybil attacks via social networks," in Proc. SIGCOMM Computer Communication Review, Sept. 2006, pp. 267– 278.

[12] H. Yu, P. Gibbons, M. Kaminski, and F. Xiao, "Sybil Limit: A near- optimal social network defense against Sybil attacks," in Proc. Symp. Security and Privacy, May 2008, pp. 3–17.

[13] Z. Li, W. Xu, R. Miller, and W. Trappe, "Securing wireless systems via lower layer enforcements," in Proc. Wkshp. Wireless Security, Sept. 2006, pp. 33–42.

[14] A. Haeberlen, E. Flannery, A. M. Ladd, A. Rudy’s, D. S. Wallach, and L. E. Kavraki, "Practical robust localization over large-scale 802.11 wireless networks," in Proc. Int. Conf. Mobile Computing and Networking, Sept. 2004, pp. 70–84.

[15] L. Xiao, L. J. Greenstein, N. B. Mandayam, and W. Trappe, "Channel-based detection of Sybil attacks in wireless networks," IEEE Trans. Information Forensics and Security, vol. 4, no. 3, pp. 492–503, Sept. 2009.

[16] D. B. Faria and D. R. Cheri ton, "Detecting identity-based attacks in wireless networks using signal prints," in Proc. Wkshp. Wireless Security, Sept. 2006, pp. 43–52.

[17] M. Demirbas and Y. Song, "An RSSI-based scheme for Sybil attack detection in wireless sensor networks," in Proc. Int. Symp. on a World of Wireless, Mobile, and Multimedia, June 2006, pp. 564–570.

[18] Y. Chen, J. Yang, W. Trappe, and R. P. Martin, "Detecting and localizing identity-based attacks in wireless and sensor networks," IEEE Trans. Vehicular Technology, vol. 5, no. 5, pp. 2418–2434, June 2010.

[19] T. Suen and A. Yasinsac, "Peer identification in wireless and sensor networks using signal properties," in Proc. Int. Conf. Mobile Ad hoc and Sensor Systems, Nov. 2005, pp. 826–833.

[20] S. Lv, X. Wang, X. Zhao, and X. Zhou, "Detecting the Sybil attack cooperatively in wireless sensor networks," in Proc. Int. Conf. Computational Intelligence and Security, Dec. 2008, pp. 442–446.