IJCOT -Special Issue– The Malla Reddy National Conference on Information System and Knowledge Engineering (MRNC-ISKE 2013) - July 2013

Trajectory Based Sybil Attacks Detection for Vehicular Ad-hoc Networks

T.Gokul Chakravarthy*1, M.Rajyalakshmi*2, D.Srujan Chandra Reddy*3

M.Tech (CSE) Student, Dept of CSE, PBRVITS, Kavali, D.t: Nellore, A.P, India

Associate Professor, Dept of CSE, PBRVITS, Kavali, D.t: Nellore, A.P, India

Associate Professor, HOD, Dept of CSE, PBRVITS, Kavali, D.t: Nellore, A.P, India

ABSTRACT:

Large-scale peer-to-peer systems face security threats from faulty or hostile remote computing elements. To resist these threats, many such systems employ redundancy. However, if a single faulty entity can present multiple identities, it can control a substantial fraction of the system, thereby undermining this redundancy. One approach to preventing these “Sybil attacks” is to have a trusted agency certify identities. This paper shows that, without a logically centralized authority, Sybil attacks are always possible except under extreme and unrealistic assumptions of resource parity and coordination among entities. Mobility is often a problem for providing security services in ad hoc networks. In this paper, we show that mobility can be used to enhance security. Specifically, we show that nodes that passively monitor traffic in the network can detect a Sybil attacker that uses a number of network identities simultaneously. We show through simulation that this detection can be done by a single node, or that multiple trusted nodes can join to improve the accuracy of detection. We then show that although the detection mechanism will falsely identify groups of nodes traveling together as a Sybil attacker, we can extend the protocol to monitor collisions at the MAC level to differentiate between a single attacker spoofing many addresses and a group of nodes traveling in close proximity.

I.INTRODUCTION:

Numerous protocols exist for forming ad hoc networks among cooperative mobile, radio-equipped nodes [2]. Many ad hoc routing protocols have been secured using reputation schemes [3] or threshold security schemes [5] that rely on there being a limited number of attackers in the group and that assume each radio represents a different individual. However, the broadcast nature of radio allows a single node to pretend to be many nodes simultaneously by using many different addresses while transmitting. This attack, an example [2] of what is called the Sybil attack [1], can easily defeat reputation [9] and threshold [10] protocols intended to protect against it. Douceur has shown that there is no practical defense against the attack; even a central authority (such as a PKI) must ensure that each identity is actually one entity—this requires costly manual intervention, which restricts the number of identities that can be managed. In contrast, protocols for detection do not suffer from such limitations. Moreover, detection is complementary to any method that attempts protection. In this paper, we show that the mobility of nodes in a wireless network can be used to detect and identify nodes that are part of a Sybil attack. We rely on the fact that while individual nodes are free to move independently, all identities of a single Sybil attacker are bound to a single physical node and must move together. We propose two initial methods, both passive, that can be run on

standard, inexpensive equipment without any special antennae or hardware and with only very loose clock synchronization. In the first method, called Passive Ad hoc Sybil Identity Detection (PASID), a single node can detect Sybil attacks by recording the identities, namely the MAC or IP addresses of other nodes it hears transmitting. Over time, the node builds a profile of which nodes are heard together, which helps reveal Sybil attackers? We show through simulation that in networks with sufficient connectivity and mobility PASID can produce close to 100% accuracy in identifying the various attacker identities while avoiding any false positives. As the network becomes more dense, with more nodes in less space, the false positive rate increases; as it becomes more sparse, the accuracy rate declines as each node has fewer chances to hear its neighbors. To combat this, we show that multiple trusted nodes can share their observations to increase the accuracy of detection over a shorter time or in a more-sparsely connected network. Our second method, PASID with Group Detection (PASID-GD), extends our approach and reduces false positives that can occur when a group of nodes moving together is falsely identified as a single Sybil attacker. By monitoring collisions at the MAC level we show that we can differentiate these cases. This approach is successful because an attacker operating over a single channel can transmit only serially, whereas independent nodes can transmit in parallel, creating detectably higher collision rates. Peer-to-peer systems commonly rely on the existence of multiple, independent remote entities to mitigate the threat of hostile peers. Many systems [3, 4, 8, 10] replicate computational or storage tasks among several remote sites to protect against integrity violations (data loss). Others [5] fragment tasks among several remote sites to protect against privacy violations (data leakage). In either case, exploiting the redundancy in the system requires the ability to determine whether two ostensibly different remote entities are actually different. If the local entity has no direct physical knowledge of remote entities, it perceives them only as informational abstractions that we call identities. The system must ensure that distinct identities refer to distinct entities; otherwise, when the local entity selects a subset of identities to redundantly perform a remote operation, it can be duped into selecting a single remote entity multiple times, thereby defeating the redundancy. We term the forging of multiple identities a Sybil attack [3] on the system.

It is tempting to envision a system in which established identities vouch for other identities, so that an entity can accept new identities by trusting the collective assurance of multiple (presumably independent) signatories, analogous to the PGP web of trust [3] for human entities. However, our results show that, in the absence of a trusted identification authority (or unrealistic assumptions about the resources available to an attacker), a Sybil attack can severely compromise the initial generation of identities, thereby undermining the chain of vouchers. Identification authorities can take various forms, not merely that of an explicit certification agency such as VeriSign [3]. For example, the CFS cooperative storage system [8] identifies each node (in part) by a hash of its IP address. The SFS network file system [2] names remote paths by appending a host identifier to a DNS name. The EMBASSY [2] platform binds machines to cryptographic keys embedded in device hardware. These approaches may thwart Sybil attacks, but they implicitly rely on the authority of a trusted agency (such as ICANN [9] or Wave Systems [5]) to establish identity.

II. RELATED WORK

The Sybil attack can occur in a distributed system that operates without a central authority to verify the identities of each communicating entity [10]. Because each entity is only aware of others through messages over a communication channel, a Sybil attacker can assume many different identities by sending messages with different identifiers. An entity in the system can attempt to determine if some set of entities are distinct by testing their resource limits, but this is problematic. If a single Sybil attacker pretends to be multiple entities, it may not have the same computational, storage, and bandwidth capabilities as multiple independent entities. However, testing based on such an assumption requires an accurate model of the attacker's resources. A Sybil attacker that has more resources than expected can impersonate a number of entities proportional to the amount its resources are underestimated. Similarly, a set of entities that are more resource-constrained than expected may fail to prove their independence. The testing entity might also attempt to verify identity and independence indirectly by asking entities to vouch for each other. This strategy is prone to the Sybil attack because multiple entities can be the multiple identities of one or more Sybil attackers. Newsome, et al [2] proposed several methods for detecting Sybil entities in a sensor network. They present an excellent discussion of the threat the Sybil attack poses to sensor networks, all of which apply to routing for ad hoc mobile networks. In contrast to the methods we propose, the detection techniques they proposed are active tests that require the participation of the neighboring nodes by asking them to respond to queries on assigned channels or to carry pre-distributed keys. Such query/response resource tests are a challenge to undertake in a mobile environment where neighbors legitimately may change with great frequency and without notice. Pre-distributing keys in an ad hoc network may not be possible if the nodes to not originate from the same source or are not all present for a key initialization phase. Regardless, a reliance on keys to detect or prevent a Sybil attack is based on a significant assumption: that each entity has been assigned exactly one key, which is difficult to ensure in practice in general, as we discuss below. Our methods of detecting Sybil attackers are related to malicious attacks against anonymous routing protocols [9] called intersection attacks [1]. Anonymous routing protocols allow an identity to remain indistinguishable from other nodes in the system. An attacker that wishes to determine the identity of an initiator can track the membership of the group over time. Each time the attacker identifies a message, it records the group membership. As membership changes due to nodes joining or leaving the group purposely or because of network failures, the intersection of all the recorded memberships converges to only the initiator. Our work in this paper is an application of the intersection attack applied to geographic location in an ad hoc network. Similarly, a Sybil attacker wishes to keep her multiple identities are indistinguishable from others in the system. However, there are differences between a Sybil attacker and legitimate nodes in a mobile wireless scenario, particularly in that independent nodes are mobile but the identities of a Sybil node move together. This provides the opportunity to identify a Sybil attacker using a location based intersection mechanism because the Sybil identities will always be part of the intersected group.

In the remainder of this section, we present an overview of the security problems that the Sybil attacks pose to ad hoc networks in particular.

III. Sybil Attacks in Ad hoc Networks

An ad hoc network is composed of mobile, wireless devices, referred to as nodes, that communicate only over a shared broadcast channel. An advantage of such a network is that no

fixed infrastructure is required: a network for routing data can be formed from whatever nodes are available. Nodes forward messages for each other to provide connectivity to nodes outside direct broadcast range. Ad hoc routing protocols are used to find a path end-to end through the cooperative network [25, 14]. Each node needs a unique address to participate in the routing. Often addresses are assigned as an IP addresses or a unique media access channel (MAC) address. Because all communications are conducted over the broadcast channel, nothing but these identifiers are available to determine what nodes are present in the network. In unsecured routing protocols, such as DSR or AODV, these address-based identifiers can be easily falsified by malicious nodes, which present an opportunity for a Sybil attack. However, allowing unauthenticated address presents a series of other attacks, including route direction, spoofing, and error fabrication [2]. Our methods work whether addresses are authenticated or not, though given the wide range of attacks possible against unauthenticated networks, Sybil attacks may not be the most significant problem present. Our methods will also work on disruption tolerant networks, however, just as such networks incur an extreme routing delay, there will be a corresponding large delay in successful sybil attack detection. Secured ad hoc networks can be classified into three broad groups, each of which can be susceptible to the

IV. Sybil attack.

• PKI-based protocols. Much of the initial work in ad hoc network security focuses on secure routing. A variety of protocols have been proposed to counter routing attacks, some of which require a central authority or other mechanism to distribute cryptographic material to nodes in the system prior to or during deployment. Systems involving a central authority are less flexible, and installing a central authority removes the chief advantage of ad hoc networks: the ability to form spontaneously from whatever nodes are available. Allowing nodes to join without pre-distributing keys leaves a potential Sybil attack.

• Threshold-based protocols. To avoid the untenable requirement of a PKI, other protocols use threshold cryptography. In such scheme, a group of trusted nodes distributes cryptographic material only if a subset of that group agrees on the trustworthiness of new members Sybil attackers can additionally defeat schemes that rely on threshold cryptography because verifying the true number and independence of nodes in the network is difficult. If a Sybil attacker can generate identities to meet the threshold requirements it can effectively control the routing of the network.

• Reputation Schemes. Other security mechanisms for ad hoc networks include protocols for determining and maintaining reputation information about nodes in the group [3]. Each node can develop trust in the other nodes that it believes are routing correctly. The Sybil attack undermines these protocols because a node can use multiple identities to falsely vouch for or otherwise support an identity that would otherwise gain a bad reputation.

A reliance on cryptographic certificates or keys does not prevent the Sybil attack in general because one entity may be in possession of multiple keys. For example, if PKI credentials are simply purchased (e.g., through VeriSign), the PKI is reduced to a resource test of each identity's wealth, which can be without bound. Unfortunately, implementing a stronger approach is problematic. This is because in practice it is untenable to create a foolproof system that can scale to a significant number of users to check identities for independence before the keys are issued. Deploying a fool

proof systems touches on issues including physical security and attacks involving social engineering or physical force. It would require checking a person against some set of unforgeable documents; but even government issued documents are forged regularly.

V. Detecting the Sybil Attack

The identities established by a Sybil attacker — whether represented by IP addresses, MAC addresses, or public keys — differ from those of an honest node in several ways. Because the resources of a single node are used to simulate multiple identities, any particular assumed identity is resource constrained in computation, storage, or bandwidth. Douecer has shown that a Sybil attacker cannot be prevented by tests of finite resources [10]. However, unlike separate entities, all identities of a Sybil attacker must share the same set of resources, and this sharing can be detected in some scenarios.

In the mobile environment, a single entity impersonating multiple identities has an important constraint that can be detected: because all identities are part of the same physical device, they must move in unison, while independent nodes are free to move at will. As nodes move geographically, all the Sybil identities will appear or disappear simultaneously as the attacker moves in and out of range. Assuming an attacker uses a single-channel radio, multiple Sybil identities must transmit serially, whereas multiple independent nodes can transmit in parallel. The latter two differences form the basis of the Sybil attack detection scheme proposed here.

VI. Formal model

As a backdrop for our results, we construct a formal model of a generic distributed computing environment. Our model definition implicitly limits the obstructive power of corrupt entities, thereby strengthening our negative results. The universe, shown schematically in Fig. 1, includes:

• A set *E* of infrastructural *entities e*

• A broadcast communication *cloud*

• A *pipe* connecting each entity to the cloud Set *E* is partitioned into two disjoint subsets, *C* and *F*. Each entity *c* in subset *C* is *correct*, abiding by the rules of any protocol we define. Each entity *f* in subset *F* is *faulty*, capable of performing any arbitrary behavior except as limited by explicit resource constraints. (The terms “correct” and “faulty” are standard in the domain of Byzantine fault tolerance, even though terms such as “honest” and “deceptive” might be more appropriate.) Entities communicate by means of *messages*. A message is an uninterrupted, finite-length bit string whose meaning is determined either by an explicit protocol or by an implicit agreement among a set of entities. An entity can send a message through its pipe, thereby broadcasting it to all other entities. The message will be received by all entities within a bounded interval of time. Message delivery is guaranteed, but there is no assurance that all entities will hear messages in the same order. This model has two noteworthy qualities: First, it is quite general. By leaving the internals of the cloud unspecified, this model includes virtually any interconnection topology of shared segments, dedicated links, routers, switches, or other components. Second, the environment in this model is very friendly. In particular, in the absence of resource constraints, denial-of-service attacks are not possible. A message from a correctly functioning entity is guaranteed to reach all other correctly functioning entities. We place a minimal restriction on the relative computational resources available to each entity, namely that there exists some security parameter *n* for which all entities can perform operations whose computational complexity is (low-order) polynomial in *n* but for which no entity can

Perform operations that are super polynomial in *n*. This restriction allows entities to use public-key cryptography to establish virtual point-to point communication paths that are private and authenticated. Although these virtual paths are as secure as point-to-point physical links, they come to exist only when created by pairs of entities that have acknowledged each other. Our model excludes direct links between entities because a physical link provides a form of centrally supplied identification of a distinct remote entity. Also, in the real world, packets can be sniffed and spoofed, so the base assumption of a broadcast medium (augmented by cryptography) is not unrealistic. An *identity* is an abstract representation that persists across multiple communication events. Each entity *e* attempts to *present* an identity *i* to other entities in the system. (Without loss of generality, we state our results with respect to a specific local entity *l* that is assumed to be correct.) If *e* successfully presents identity *i* to *l*, we say that *l accepts* identity *i.*

A straightforward form for an identity is a secure hash of a public key. Under standard cryptographic assumptions, such an identifier is unforgeable. Furthermore, since it can generate a symmetric key for a communication session, it is also persistent in a useful way. Each correct entity *c* will attempt to present one *legitimate* identity. Each faulty entity *f* may attempt to present a legitimate identity and one or more *counterfeit* identities. Ideally, the system should accept all legitimate identities but no counterfeit entities.

VII. Conclusion

In this paper, we have presented the first completely passive approach to detecting a Sybil attacker in a network. PASID detects which network identities are related and likely to belong to the same Sybil attacker by monitoring what identities seem to be physically located together, and it can achieve 90% or more accuracy with no false positives in some circumstances. Adding additional observer nodes increases the accuracy to 100% and increases the range over which this accuracy is possible. We also have shown that PASID will detect a group of nodes moving together as a Sybil attacker, and we presented an extension to the method called PASID-GD that monitors collisions at the MAC level to differentiate between the single Sybil attacker and a group moving together.

Peer-to-peer systems often rely on redundancy to diminish their dependence on potentially hostile peers. If distinct identities for remote entities are not established either by an explicit certification authority (as in Farsite [3]) or by an implicit one (as in CFS [8]), these systems are susceptible to Sybil attacks, in which a small number of entities counterfeit multiple identities so as to compromise a disproportionate share of the system.

VIII. References

[1] T. Aura, P. Nikander, J. Leiwo, "DoS-Resistant Authentication with Client Puzzles", *Cambridge Security Protocols Workshop*, Springer, 2000.

[2] M. Bellare and P. Rogaway, "Random Oracles are Practical: A Paradigm for Designing Efficient Protocols", *1st Conference on Computer and Communications Security*, ACM, 1993, pp. 62-73.

[3] W. J. Bolosky, J. R. Douceur, D. Ely, M. Theimer, "Feasibility of a Serverless Distributed File System Deployed on an Existing Set of Desktop PCs", *SIGMETRICS 2000*, 2000, pp. 34-43.

[4] M. Castro, B. Liskov, "Practical Byzantine Fault Tolerance", *3rd OSDI*, 1999.

[5] D. Chaum, "Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms", *CACM* 4 (2), 1982.

[6] B. Chor, O. Goldreich, E. Kushilevitz, M. Sudan, "Private Information Retrieval", *36th FOCS*, 1995.

[7] I. Clarke, O. Sandberg, B. Wiley, T. Hong, "Freenet: A Distributed Anonymous Information

Storage and Retrieval System", *Design Issues in Anonymity and Unobervability*, ICSI, 2000.

[8] F. Dabek, M. F. Kaashoek, D. Karger, R. Morris, I. Stoica, "Wide-Area Cooperative Storage with CFS", *18th SOSP*, 2001, pp. 202-215.

[9] D. Dean, A. Stubblefield, "Using Client Puzzles to Protect TLS", *10th USENIX Security Symp.*, 2001.

[10]R. Dingledine, M. Freedman, D. Molnar "The Free Haven Project: Distributed Anonymous Storage Service", *Design Issues in Anonymity and Unobservability*, 2000.