Investigating the Learning Phase of an Autonomous Authentication in Mobile Ad-hoc Networks

Hang Zhang
University of Göttingen
hang.zhang@cs.uni-goettingen.de

Parisa Memarmoshrefi
University of Göttingen
memarmoshrefi@informatik.uni-goettingen.de

Fatemeh Ashrafi
University of Göttingen
fatemeh.ashrafi@stud.uni-goettingen.de

Dieter Hogrefe
University of Göttingen
hogrefe@cs.uni-goettingen.de

ABSTRACT

In this work we focus on investigating the learning phase of an autonomous authentication mechanism. Through a series of simulation, an experimental best cutoff point and the aggression threshold values for different network size were calculated. In the test phase, those found values are proved by the average good accuracy.

Categories and Subject Descriptors

C.2.7 [**Networks Security**]: Mobile and wireless security

General Terms

Security, Performance, Design.

Keywords

Aggression/distrust, Public key certificate chain, Attacker, Ad-hoc networks.

1. INTRODUCTION

In a fully distributed wireless Mobile Ad-hoc Networks (MANETs), a security mechanism is often in a self-organized manner. Among security services, authentication is the most important service that ensures confidentiality, integrity and access control. Self-organizing generally is used for dynamic systems consisting of individuals where interaction between individuals leads to a global pattern, intelligence or behavior. In regard to multi-hop and dynamic topology characteristics in MANETs, performing authentication process by a single trusted party is not feasible. One proposed mechanism [1] is to enable each node to create their public/private key pairs and make their public key available, while keeping the private key secrete. A serious problem in most self-organizing authentication mechanism is to create a web of trust based on the observed behaviors of the individuals in the network. This trust model leaves decision making on trustworthiness of the public keys in the hand of nodes. However, with the lack of central fully trusted center, there is no guarantee to certify the authenticity of the nodes in the network. Attack occurs when a node can bind its key pairs to the identity of another entity and pretend to act as the victim party. Therefore, it is essential to confirm a particular public key which correctly belongs to an entity it claims. Generally in a self-organized networks system each individual needs a learning phase to verify the certificates, as there is no central certificate authority. In this work we focus on investigating the learning phase of a bio-inspired authentication mechanism [2].

2. ACO-BASED CERTIFICATION MECHANISM

In the authentication scheme, each node in the self-organized network works autonomously as a certificate authority. The node generates a public and private key pair for itself and uses its private key for issuing certificates to its direct neighboring nodes. As illustrated in Fig.1, once a source node S wants to make a secure communication with a non-neighbor node e.g. node D, S needs to find a certificate chain from S to D which reports/vouches for D's public key. However, the correctness of the reported D's public key is not guarantee

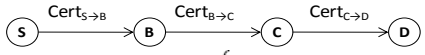

Figure 1. PK certificate chain: $\{Cert_{S\to B}, Cert_{B\to C}, Cert_{C\to D}\}$

The attacker can issue a fake certificate for the target node and sends it back to source node. In order to gather information about the behavior of other nodes, source nodes start to request the public keys of some randomly chosen destination nodes in the network. For each public key (PK) request, the source node S sends out some forward ants (FA) toward destination. When a FA reaches to the destination node, it is transformed into a backward ant (BA) and the BA retraces exactly the same path of the FA back to the source node S. Along its journey, BA carries all the certificates of the intermediate nodes in the path. After receiving all the BAs or if the PK discovery timeout occurs, node S begins the analysis phase.

3. LEARNING PHASE

3.1 Similarity Nodes' Behavior

In the analysis phase, first, the source node extracts the features of nodes involved in the different received certificate chains. It builds the objects matrix and applies Hierarchical Cluster Analysis (HCA) to cluster the nodes Based on the nodes' behavior

BICT 2015, December 03-05, New York City, United States

DOI 10.4108/eai.3-12-2015.2262465

similarity. Once the cluster tree is built, a cutoff point needs to be found to discriminate the normal nodes from the potential attacker nodes who transfer a fake certificate of the target destination node. In order to determine the best cutoff point, experimentally the tree was cut with different cutoff points. The point that classifies nodes into honest and attacker classes which is most matched to the real attacker/honest nodes in the network, is considered as the best cutoff point. Nodes with dissimilar behavior classified in different groups and lead to have more aggression/distrust toward each other [2]. In the learning phase, 360 scenarios were performed in QualNet. In the base scenario, 30 nodes were randomly distributed in an open area. 20% of the nodes were chosen as source nodes. Each of them sends out some number of ants to sequentially discover the public keys of 4 different destination nodes. The whole simulation time is set to 100s. A series of scenarios were considered under different networking conditions by varying the network size, the node's speed and the malicious nodes percentage in the network.

Table 1. Some other simulation parameters

Parameter	Value
Network size	30,40 and 50
Open area size (m^2)	1500^2, 1732^2 and 1936^2
Node's mobility (m/s)	0, 5 and 10
Attacker nodes' percentage	Up to 20%

3.2 Parameter Settings

3.2.1 Cut-off Calculation

The best cluster tree cut point is the point that leads the highest aggression/distrust value for attacker nodes. The results from 360 runs indicated that the best cut-off point was approximately 0.804 for 30 nodes; 0.7807 for 40 nodes and 0.7667 for 50 nodes.

3.2.2 Aggression threshold

The aggression/distrust threshold value is lowest aggression value which indicates whether a node is considered as an attacker. From the experiments, the lowest average aggression threshold values to discriminate attacker nodes was 0.2 for 30 nodes, 0.3 for 40 nodes and 0.2 for 50 nodes. Fig.2 demonstrates that the average aggression/distrust values in networks with higher speed nodes increased in compare to static and lower speed networks. We reason that nodes in networks with higher mobility encounter faster with each other which leads to get the information about their environment faster.

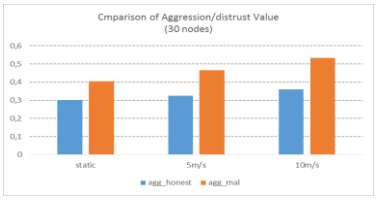

Figure 2. Average aggression/distrust value toward the honest and attacker nodes in the network

4. EVALUATION

In the test phase, 360 new scenarios were performed. Based on the observation from learning phase, an approximate average best cutoff with 0.79 was applied for the test phase. Fig.3 indicates that moving nodes have a general better accuracy for attacker nodes detection. Fig.4 shows that, the true positive rate generally reduces from 0.98 when the network size rises, however it maintains above 0.80 in the worst case. The results are averaged over all malicious percentages.

5. CONCLUSION AND FUTURE WORK

In this work, the learning phase of an ACO-based autonomous authentication model was investigated. Through a series of simulations, an experimental best cutoff point and the aggression threshold values for different network size were identified. In the test phase, those founding values are proved by the average good accuracy. For the next step, we will feed the calculated parameters to QualNet simulator and let the autonomous authentication running; and via trust and aggression/distrust values updating enable nodes to make a secure communication with a target node upon retrieving its correct PK.

6. REFERENCES

[1] Memarmoshrefi, P., Seibel, R., and Hogrefe, D., 2012. Bio-inspired Self-organized Public Key Authentication Mechanism for Mobile Ad-hoc Networks, Bio-Inspired Models of Network, Information, and Computing Systems. In 5th International ICST Conference, BIONETICS 2010, Boston, USA, 375-386

[2] Memarmoshrefi, P., Zhang, H., and Hogrefe, D., 2014. Social insect-based sybil attack detection in mobile ad-hoc networks. In Proceedings of the 8th International Conference on Bioinspired Information and Communications Technologies (BICT '14). ICST, Brussels, Belgium, Belgium, 141-148.

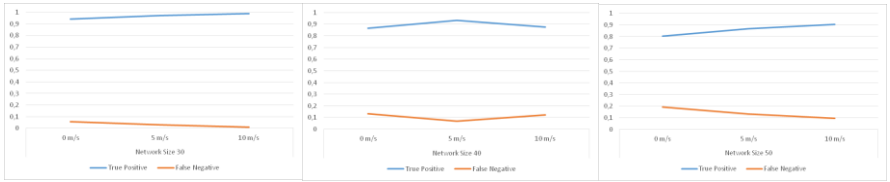

Figure 3. Compare true positive & false negative trends based on network size

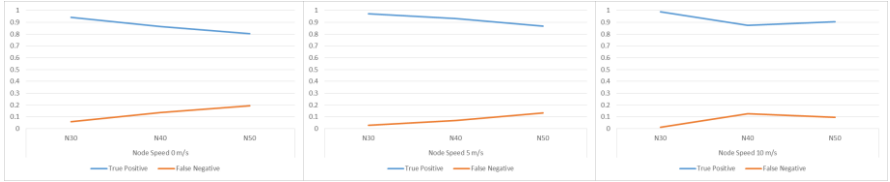

Figure 4. Compare true positive & false negative trends based on node speed