

POSTER: Bio-Inspired Distributed Certificate Revocation in Vehicular Ad Hoc Networks

Anvay Lonkar
Department of Information Technology
Delhi College of Engineering
anvay.lonkar@gmail.com

Ankur Khetrapal
Department of Computer Engineering
Delhi College of Engineering
ankur.khetrapal@gmail.com

ABSTRACT

As one of the most dynamic and gigantic instantiations of the Mobile Ad Hoc Networks, VANET's have attracted a lot of research towards the scalability of security aspects. Most results tend to point towards a digital signature based Public Key Encryption mechanism. Intermittent access to the fixed infrastructure, especially during the initial stages of deployment, makes certificate management a core issue in all such research activities. In this paper we propose swarm intelligence based temporal certificate revocation information dissemination mechanism for robust and efficient detection and certificate revocation of malicious (or anomalous) nodes. We use the Ant colony optimization as a metaheuristic optimization algorithm to find a globally optimal solution for distributing certificate revocation information to the nodes that need it most. Our simulation results show lower latencies for prohibition of malicious nodes from the network.

1. INTRODUCTION

Vehicular Ad Hoc networks have been envisioned to provide various services which include collision avoidance, providing information on road and traffic conditions, local tourist information, platooning etc. These services depend on a vehicle communicating with other vehicles and the road side infrastructure (RSI). As these services grow and need grows for them to become more secure (eg. financial transactions), security aspects become increasingly important for VANET's. Huge amount of research has already gone into making VANET's more secure [1] [2] etc. Various schemes (reputation systems etc.) have been proposed to this end. But the increased mobility and possibly high network usage require highly efficient algorithms to manage the authenticity of communicating nodes.

Past research [2] [3] suggest PKI (Public Key Infrastructure) with Digital Signatures as the most suitable method for securing communication amongst nodes in VANETS. This requires the existence of Certifying Authority (CA) (Also referred to as Trusted Third Party – TTP in [3]) whose job is to issue and manage Digital Certificates. Assuming this as our basic scheme (same as assumed by [4]) we work on how to revoke certificates of malicious nodes in an environment where access to the CA is not possible. Other tasks to be performed by the CA have been thoroughly researched and hence this certificate revocation aspect is acting as a bottleneck in efficient and secure aggregation of information.

We use the swarm intelligence approach to propose an optimized algorithm for certificate revocation in a distributed environment. We demonstrate preliminary simulation results to show how lower latencies are confronted in spreading the information about the

maliciousness of a particular node to other nodes within the transmission region.

The rest of the paper is organized as follows: Section 2: describes the basics of the swarm intelligence approach; Section 3 describes our algorithm; Section 4 provides a preamble to our simulation results and we conclude in Section 5.

2. SWARM INTELLIGENCE

The Swarm Intelligence Paradigm [9] comprises of the ant-based colony optimization algorithm that is widely used to solve various dynamic combinatorial optimization problems. The basic principle behind these algorithms is a concept called *stigmergy* - communicating through the environment. As an example, ants drop pheromones to communicate with other ants that might be following their trails. This principle is widely used in routing for networks [10]. Fig1 demonstrates how ants use this pheromone deposit paradigm in real time to find food.

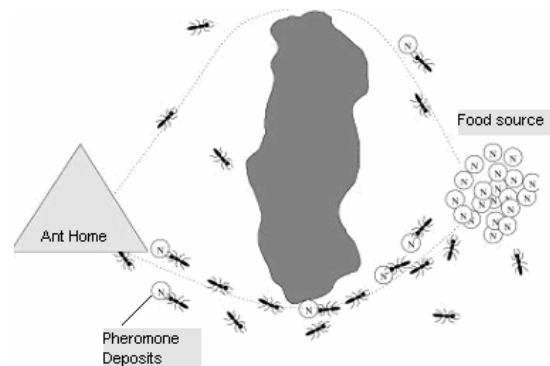


Fig1. Ants using pheromone deposits to find food

In our approach vehicular nodes interacting with each other send out ants depositing information (i.e. pheromone) regarding the maliciousness of other nodes. Then, a node establishes the authenticity of another node following a pheromone regulation process and hence aggregating all information available to the network taking an informed decision in an optimized manner.

3. ANT-BASED DISTRIBUTED CERTIFICATE REVOCATION PROTOCOL (AB-DCRP)

In our model of a VANET security system we assume the certifying authority responsible for generation and distribution of digital signatures for all nodes entering the network. This CA could be the manufacturer, an international consortium or a government body.

Once a node becomes the part of a Vehicular network it monitors the performance (including authenticity and

honesty) of other nodes using all the available sensor data. We assume this to be done by a black box [6]. Till the time it continues to be in touch with the RSI, it transmits this information back to the CA and makes it responsible for handling non-repudiation and banishing of any nodes from the network.

The problem we are trying to tackle is in the scenario when connection to the RSI is not available. This kind of a situation will occur in plenty for VANET's, especially during the early years of deployment and in rural areas. In this case a node will not be able to perform the following two jobs:

1. Request for the public key of a node that it wants to communicate with
2. Transfer information regarding the maliciousness of a node that it has detected.

Ant based request for certificates has already been proposed in [7] for MANET's and can be easily adapted for highly mobile networks like VANETS.

In addition to looking for certificates, ants can also be sent out to distribute information regarding honesty (or dishonesty) of particular nodes. Then each node, based on all information gathered through these ants, can take a decision regarding temporal revocation of certificates (till the time it comes in contact with the RSI and offloads this information to the CA) of that node. This decision can be made in a manner described in [8]. In the next sub-section we describe a mechanism for disseminating maliciousness information.

3.1 Ants for maliciousness information dissemination

As shown in Fig.2, on detection a malicious node, ants containing this information are sent out to all nodes within the communication range of the sending node. The ants travel based on a revocation table (RT) which is contained by each node. The RT (which looks similar to a distance vector routing table) holds information regarding each node and the amount of maliciousness related to that node. The ant updates this information and then travels in the direction of the node which, according to the RT, considers the accused node (B in fig 2) to be the most malicious.

When the ant reaches a node (say C_i) where the maliciousness metric (stored by the RT) reaches above a threshold value for B, then C_i revokes the certificate of B and sends out a backtracking ant to A and all other intermediate nodes informing it of his actions.

At present we use a simple linear formula to update the RT:

$$M_{C_i B} = M_{C_i B} + M_{A B} * M_{C_i A}$$

Where $M_{x y}$ is the malicious metric of y as seen by x. In the above formula the RT of C_i is being updated for B by an ant sent out by A.

4. SIMULATION

We are currently in the process of running simulations for the range of 10-30 nodes per kilometer with a single malicious node as detected by all nodes in its transmission

region. Preliminary results show that the time required for all nodes to detect a malicious node increases linearly for AB-DICRP as opposed to exponentially for a statistical revocation mechanism [8]. We use the ns-2 simulation tool.

5. CONCLUSION AND FUTURE WORK

Using a bio-inspired ant colony optimization technique we have proposed a new information dissemination protocol which can possibly reduce the latencies related to detecting malicious nodes in a distributed ad hoc vehicular environment. Future work includes deriving a second order update formula for the RT's and more in-depth testing of the current protocols on a multitude of test beds. We are also working on devising new metrics for evaluating such protocols.

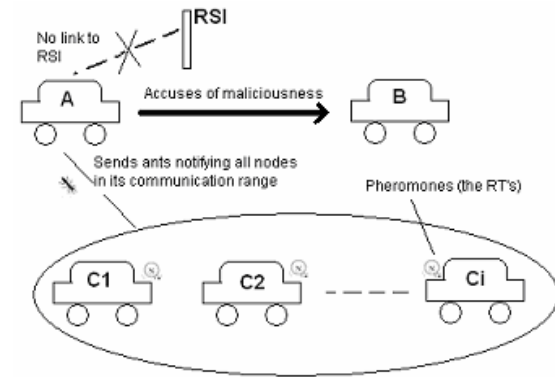


Fig2. Distributing maliciousness information using ants

REFERENCES

- [1] M. Raya, A. Aziz and J-P Hubaux. Efficient Secure Aggregation in VANETS. In VANET'06, September 29, 2006.
- [2] K. Plobl, T. Nowey, C. Mletzko. Towards a Security Architecture for Vehicular Ad Hoc Networks. Proceedings of the First International Conference on Availability, Reliability and Security (ARES'06).
- [3] M. Raya and J-P Hubaux. The Security of Vanets. In VANET'05, September 2, 2005.
- [4] E. Bonabeau, M. Dorigo, and G. Theraulaz. *Swarm Intelligence - From Natural to Artificial Systems*. Oxford University Press, New York, 1999.
- [5] Kassabalidis, I.; El-Sharkawi, M.A.; Marks, R.J., II; Arabshahi, P.; Gray, A.A. Swarm intelligence for routing in communication networks. Global Telecommunications Conference, 2001. GLOBECOM apos;01. IEEE Volume 6, Issue , 2001 Page(s):3613 - 3617 vol.6
- [6] Golle, P.; Greene, D. H.; Staddon, J. Detecting and correcting malicious data in VANETS. Proceedings of the First ACM Workshop on Vehicular Ad Hoc Networks; 2004 October 1; Philadelphia, PA. NY: ACM; 2004; 29-37.
- [7] Tao Jiang John S. Baras Ant-based Adaptive Trust Evidence Distribution in MANET*
- [8] M. Raya, A. Aziz and J-P Hubaux. Certificate Revocation in Vehicular Networks