Cognitive Security Protocol for Sensor Based VANET Using Swarm Intelligence

Rajani Muraleedharan and Lisa Ann Osadciw
Department of Electrical Engineering and Computer Science
Syracuse University, Syracuse, NY- 13244-1240
Phone: 315-443-3366/Fax: 315-443-2583
{rmuralee, laosadc}@ecs.syr.edu

Abstract

Intelligent Transportation system (ITS) using wireless and mobile ad-hoc sensor network has inspired many autonomous applications. Vehicular Ad-hoc network (VANET) is an emerging technology where vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communicate wirelessly using dedicated short-range communication band. In sensor based VANET (S-VANET) issues like response time, data aging, bandwidth, packet delivery, message prioritization and communication cost is a major concern. In this paper, we apply cognitive security protocol that disseminates information using distributed sensor technology while prioritizing prevention of data aging, efficient quality-of-service (QoS) and robustness against denial-of-service (DoS) attack. The reliability and optimality of the protocol is computed based on current mission response time and maintaining message authentication, integrity, confidentiality and non-repudiation.

1. Introduction

A growing need for automated and intelligent transportation [1] support is required to facilitate dynamic on-road assistance, emergency evacuations, etc over a vast geographic area. Current transportation support system has many shortcomings such as mobility, scalability, adaptability and cost. Devices and applications based on wireless technology promises cheap and tiny sensors that can sense information within its coverage area and relay information using multi-hops.

Sensor based vehicular ad-hoc network (S-VANET) as shown in Figure 1, enables information sensing, aggregation, dissemination, and storing within sensors and vehicles in a distributed fashion. The primary task of the S-VANET is to aggregate and facilitate information to and from all the neighboring vehicles for situation or threat assessment. Apart, from neighboring vehicular information, other data sources like passenger interest, radio, satellite, traffic management information can also be applied to improve the quality of information (QoI). Although, S-VANET promises to solve shortcomings of current technology, security has become a major concern in these applications.

Fig 1: Sensor Based Vehicular Ad-hoc Network (S-VANET) [1]

In this paper, denial-of-service (DoS) attack [2] on S-VANET is analyzed. There are many ongoing researches proposed to ensure the four major features of security, confidentiality, integrity, authenticity and authorization in S-VANET. Since S-VANET applies wireless, wired and mobile devices, security measures based on threats on individual devices needs to be considered.

2. Security Requirements in VANET

Security is a primary concern of any application, wired, wireless, ad-hoc and mobile networks. In recent years, security and privacy in sensor network and VANET has caused concerns in infrastructure and

reliability of information. A security framework for S-VANET should have the following features,

1. Optimize and balance resources at each node
2. Traffic prioritization based on situation and threat assessment
3. Improved message confidentiality, integrity, authentication and authorization (CIAA)
4. Increased information reliability and accuracy
5. Increased response time
6. Platform and device independent
7. De-centralized

2.1. Problem Statement

There are four major reasons why security is crucial in S-VANET. First, the information transmitted over a wireless channel between highly mobile nodes and vehicles is insecure and harsh environments. Second, there is no centralized control of information being transmitted over the sensor network, which threatens the users and information confidentiality and authenticity. Third, the topology of VANET is dynamic i.e. sensor network, RFID, VANET etc. Fourth, apart from outsider adversary threats, an insider attack can be easily left undetected. Vehicular sensors have unlimited power supply, but high-end security defenses will only delay application response. Thus, a security scheme requires continuous knowledge of resource availability and anomaly detection within and outside the network.

There are some basic assumptions about S-VANET. First, sensors require to be authenticated by a cluster-head formed within a time-slot, to transmit information. Second, not all vehicles or nodes are under threat i.e. k nodes compromised out of N. Third, the sensors within a sensing range have correlated data, and hence fused data is sent to sink. Fourth, any participating vehicle and node abides by the threshold settings of the S-VANET.

3. Denial-of-Service

Denial of Service (DoS) is one of the simple and most effective attacks placed by an intruder. DoS, is an act by adversary to reduce the reliability of the application. Since, no security measures are taken during the design phase, every layer of a network is prone to DoS attacks. The different types of DoS attack is based on physical, link and network, such as Jamming, Sybil and Collision attack. In this paper, we primarily concentrate on two DoS attacks, Sybil and Collision [3, 4]. These two attacks leads to packet loss, localization error and integrity of information transmitted. Due to the varied design constraints and missions in S-VANET, a nature inspired framework and optimization technique is applied.

4. Secure Nature-Inspired Framework

Selecting a path that satisfies multiple QoS constraint is Nondeterministic Polynomial (NP) Complete problem, on the other hand, optimizing load balancing based on resource priorities is a Nondeterministic Polynomial (NP) hard problem. Therefore, we require scheme that can obtain an optimal and efficient solution. There are many schemes inspired by nature, such as genetic, ant, bee, bird flocking etc. In this paper, we primarily concentrate on mimicking ant's behavior in finding a solution from its source to sink. There are three main characteristics of an ant agent, 1. Pheromone, 2. Transition Probability and 3. Tabu-list. A background on Ant System (AS) and its features can be found in [5, 6]. These characteristics help to find an optimal and secure path against Sybil and Collision attack.

The cognitive security protocol combines features of the AS and Bayesian inference to estimate an outcome based on the apriori knowledge of traffic patterns. The performance metrics, such as distance and packet delivery rate play a crucial role in detecting Sybil and Collision attack.

5. Experimental Results

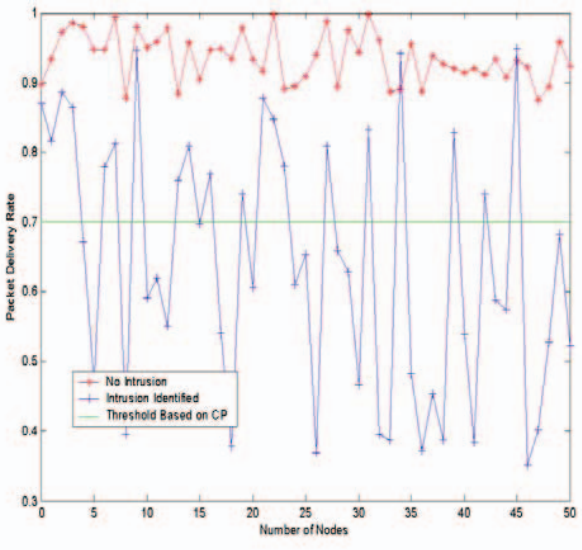

Fig 2. Nature Inspired: Intrusion Detection Using PDR metric, and Constant Threshold

In Figure 2 there are normal, intruders and threshold of packet delivery is shown. The process of identifying an intrusion is based on agent's performance metrics i.e.,

PDR, energy, BER, distance, hop stored in the tabu-list. When the agents sense a sudden change (elevation or dip) in PDR from its previous tour, it flags the node and updates globally. Depending on the weights given to each of the metric the flag is triggered.

6. References

[1] R. Muraleedharan and L.A. Osadciw, "Cognitive Routing Protocol for Sensor Based Intelligent Transportation System", in *Wireless Technologies for Intelligent Transportation Systems*, edited by Ming-Tuo Zhou, Y. Zhang and Laurence T. Yang, Nova Science Publishers, USA, 2008.

[2] A.D. Wood and J.A. Stankovic, "Denial of Service in Sensor Networks", *IEEE Computer*, Vol 35, Issue: 10, Oct 2002.

[3] J. Newsome, E. Shi, D. Song and A.Perrig, "The Sybil Attack in Sensor Networks: Analysis and Defenses", *Third International Symposium on Information Processing in Sensor Networks (IPSN)*, 2004.

[4] M. Demirbas, Y.W. Song, "An RSSI-based Scheme for Sybil attack detection in Wireless Sensor Networks", *International Workshop on Wireless Mobile Multimedia* (*WOWMOM*'06), New York, USA. 2006: 564–570.

[5] E. Bonabeau, M. Dorigo, and G. Théraulaz, "Swarm intelligence: from natural to artificial systems", *Oxford University Press*, 1999.

[6] R. Muraleedharan R and L.A. Osadciw, "A Predictive Sensor Network Using Ant Systems ", *In Proc of SPIE Defence and Security*, Orlando, Apr 12-17, 2004.