INTERNATIONAL RESEARCH JOURNAL IN ADVANCED ENGINEERING AND TECHNOLOGY (IRJAET) E - ISSN: 2454-4752 P - ISSN : 2454-4744
VOL 4 ISSUE 2 (2018) PAGES 3232 - 3238
RECEIVED : 10.03.2018 PUBLISHED : 11.04.2018
April 11, 2018

TO ENHANCE SECURITY AGAINST LETHAL CYBER-ATTACKS IN UAV NETWORKS

G.Avinash[1],R.Bharath[2],H.Karthick[3],V.Vinoth Kumar[4]

Department of Computer Science and Engineering

Students[1, 2,3] ,Assistant Professor[4]

Kingston Engineering College, Vellore, India.

ABSTRACT

Unmanned aerial vehicles (UAVs) networks have not yet received considerable research attention. Specifically, security issues are a major concern because such networks, which carry vital information, are prone to various attacks. In this paper, we design and implement a novel intrusion detection and response scheme, which operates at the UAV and ground station levels, to detect malicious anomalies that threaten the network. In this scheme, a set of detection and response techniques are proposed to monitor the UAV behaviors and categorize them into the appropriate list (normal, abnormal, suspect, and malicious) according to the detected cyber-attack. We focus on the most lethal cyber-attacks that can target an UAV network, namely, false information dissemination, GPS spoofing, jamming, and black hole and gray hole attacks. Extensive simulations confirm that the proposed scheme performs well in terms of attack detection even with a large number of UAVs and attackers since it exhibits a high detection rate, a low number of false positives, and prompt detection with a low communication overhead.

1. INTRODUCTION

AVEHICULAR network is a network of vehicles which communicate with each other via short-range wireless communications. Vehicles can therefore communication with each other either directly when there meet each other or through multi hop transmissions. Vehicles can act as powerful sensors and form mobile sensor networks. Vehicular networks have many appealing applications, such as driving safety, intelligent transport, infrastructure monitoring, and urban monitoring. Today 3G networks are getting more and more popular and ubiquitous access to 3G is possible. Moving vehicles can also communicate with each other via 3G. The 3G communication has advantage of ubiquitous access and shorter delay. Compared with multi hop inter-vehicle communication, however, communication via 3G has limitations. First, although 3G communications becomes more and more cheap, the cost of 3G communication is still high. In Shanghai, China, for example, the rate of 3G data communication is around 1 USD for only 30 MByte. By contrast, ad hoc vehicular communication is for free. Second, the bandwidth of inter-vehicle communication, realized through DSRC or 802.11, can be higher than that of 3G. Finally, many real-time applications, e.g., emergent message dissemination, are time critical and direct inter-vehicle communications may be more suitable.

Efficient inter-vehicle data delivery is of central importance to vehicular networks and such importance has been recognized by many existing studies. In this paper we focus on such vehicular networks that are sparse and do no assume that all vehicles on the road are member nodes of the vehicular network. Such sparse vehicular networks feature infrequent communication opportunities. Inter-vehicle data delivery may introduce non negligible delivery latency because of frequent topology disconnection of a vehicular network. Thus, we should stress that the inter-vehicle communication in vehicular network are suitable for those applications which can tolerate certain delivery latency. For example, in the context of urban sensing, vehicles continuously collect useful information, such as road traffic conditions and road closures. A vehicle may send a query for a specific kind of information and the one that has the information should respond the querying node with the data. Such communications require multi-hop data delivery in vehicular networks. Other examples of such applications include peer-to-peer file sharing, entertainment, advertisement, and file downloading.

There is a great deal of uncertainty associated with vehicle mobility. Vehicles move at their own wills. It is difficult, if not impossible, to gain the complete knowledge about the vehicular trace of future movement, i.e., the position of the vehicle at a given point in time. For routing in a vehicular network, a relay node must decide how long a packet should be kept and which node a given packet should be forwarded to. Existing study shows that it is possible to find an optimal routing path when the knowledge of future node traces is available, which is NP-hard though? However, it is impractical to have prior knowledge about future traces of nodes. The knowledge of future vehicular trajectories plays a key role for optimal data delivery. Existing routing algorithms heavily rely on prediction of vehicle mobility. However, they have adopted only simple mobility patterns, such as the spatial distribution and inter-meeting time distribution, which support coarse-grained predictions of vehicle movements. Some algorithms assume random mobility in which vehicles move randomly in an open space or a road network. This model is simple but far from the reality. Some other algorithms assume simple mobility patterns such as exponential inter-meeting times and regular spatial distributions. As a result, prediction results based on these simple patterns are of limited value to efficient data delivery in vehicular networks. In addition, many of existing algorithms ignore the fact that links in a vehicular network have unique characteristics. On the one hand, a link is typically short-lived. This suggests that the capacity of the link is limited. Thus, the order for forwarding packets becomes important. On the other hand, links in a densely populated area may interfere with each other. This indicates that link scheduling becomes necessary.

To overcome the limitations of existing algorithms, this paper proposes an approach to exploiting the hidden mobility regularity of vehicles to predict future trajectories. By mining the extensive data set of vehicular traces from more than 4,000 taxis in Shanghai, China, we show that there is strong spatiotemporal regularity with vehicle mobility. More specifically, our results based on conditional entropy analysis demonstrate that the future trajectory of a vehicle is greatly correlated with its previous trajectory. Thus, we develop multiple order Markov chains for predicting future trajectories of vehicles. With the available future trajectories of vehicles, we propose an analytical model and theoretically derive the delivery probability of a packet.

Since the optimal routing problem with given vehicle trajectories is still NP-hard, we develop an efficient global algorithm for computing routing paths when predicted trajectories are available. For more practical situations, we develop a fully distributed algorithm which needs only localized information. The two algorithms jointly consider packet scheduling and link scheduling. We evaluate the algorithms with extensive trace driven simulations, based on the trace data set collected in Shanghai and Shenzhen. The results demonstrate that our algorithm onsiderably outperforms other algorithms in terms of delivery probability and delivery efficiency.
Input Design is the process of converting a user-oriented description of the input into a computer-based system. This design is important to avoid errors in the data input process and show the correct direction to the management for getting correct information from the computerized system.

It is achieved by creating user-friendly screens for the data entry to handle large volume of data. The goal of designing input is to make data entry easier and to be free from errors. The data entry screen is designed in such a way that all the data manipulates can be performed. It also provides record viewing facilities. A large body of works considers the problem of preserving the user's privacy in the context of location based services (LBSs). For instance, the middle layer of DSRC defines the security services for application and message management. Authentication schemes are designed to preserve the driver privacy in DSRC-based VANETs. To prevent malicious tracking, a vehicle could change its anonymous key within an interval of a few minutes. DIVERT has a different goal from all these works: it focuses on protecting the driver's location privacy from the central server, not from the other drivers in vehicle ad hoc network. For driver-to-driver privacy, DIVERT can leverage the existing solutions.

2. EXISTING SYSTEM

The proposed hierarchical detection and response scheme is running at the UAV and ground station levels to detect any malicious anomalies that threaten the network. To achieve high accuracy, the hierarchical scheme combines rules-based detection and anomaly detection techniques. With the help of these detection techniques, we also develop a new response scheme that categorizes the monitored UAVs into appropriate lists (normal, suspect, abnormal, and malicious) according to their behaviors. Our IDS-based solution achieves the following Characteristics. Smart activation of the intrusion monitoring process: in fact, when a large number of nodes launch their monitoring processes, the incurred overhead can be substantial Therefore, a tradeoff between the intrusion detection rate and overhead is considered in this paper.

3. PROPOSED SYSTEM

A number of DTN mechanisms have been proposed to address communications disconnections and improve the network delay. In this paper, inspired by the DTN routing protocol proposed by we propose to use a ground station as a relay node when the next-hop UAV is not available. Note that the ground station could be for instance an emergency vehicle and is part of the network. These kinds of vehicles are assumed to be relatively static since they are not mobile in case of disasters; they are quickly deployed and remain stationary for a relatively long period of time in, e.g., hours or days. In addition, they are assumed to be trusted nodes, and possess higher computational capabilities as compared to UAVs. We propose and conceive in this paper an efficient and lightweight detection and response scheme

to protect UAV networks. This system is efficient since it detects the attacks promptly and it is lightweight because it requires a low overhead to achieve a high level of security (i.e., high detection and low false positive rates). The malicious node that executes a DoS attack attempts to exhaust energy resources of UAVs or disturb the network and routing protocol. Jamming and gray hole and black hole attacks are among the major lethal DoS attacks.

ADVANTAGES

Attack detection even with large number of UAVs and attackers.It exhibits a high detection rate.A low number of false positives and prompt detection with a low communication overhead.

DISADVANTAGES

Lethal cyber-attacks that can target an UAV network.GPS spoofing,jmming,and black hole and gray hole attacks are more.

4. LITERATURE SURVEY

Efficient Data Dissemination in Cooperative Vehicular Networks

Vehicular Networks are drawing the attention of both research community and automotive industry since they provide Intelligent Transportation Systems (ITS) as well as drivers and passengers' assistant services. However, the industrialization of such networks faces a number of challenges, in particular the high cost of the infrastructure to deploy. To overcome this problem, an effective solution is to rely on cooperative vehicle-to-vehicle (V2V) communication to minimize the deployed infrastructure. Since, a large number of Cooperative V2V applications are broadcasting by nature, we proposed an efficient dissemination protocol: ROD (Road Oriented Dissemination). ROD consists in two modules: (i) Optimized Distance Defer Transfer module, and (ii) Store and Forward module. We compare our protocol to other dissemination protocols and analyze its performances by simulations, on-road tests and analytically. Performance study shows interesting results of ROD compared to the other existing solutions. ROD is able to provide a low end-to-end delay, a high delivery ratios and a minimum bandwidth usage since only a limited number of vehicles are involved in the broadcast scheme.

On the Security of the Automatic Dependent Surveillance-Broadcast Protocol

Automatic dependent surveillance-broadcast (ADSB) is the communications protocol currently being rolled out as part of next generation air transportation systems. As the heart of modern air traffic control, it will play an essential role in the protection of two billion passengers per year, besides being crucial to many other interest groups in aviation. The inherent lack of security measures in the ADS-B protocol has long been a topic in both the aviation circles and in the academic community. Due to recently published proof-of-concept attacks, the topic is becoming ever more pressing, especially with the deadline for mandatory implementation in most airspaces fast approaching. This survey first summarizes the attacks and problems that have been reported in relation to ADS-B security. hereafter, it surveys both the theoretical and practical efforts which have been previously conducted concerning these issues, including possible countermeasures. In addition, the survey seeks to go beyond the current state of the art and gives a detailed assessment of security measures which have been developed more generally for

related wireless networks such as sensor networks and vehicular ad hoc networks, including taxonomy of all considered approaches.

Adaptive Intrusion Detection of Malicious Unmanned Air Vehicles Using Behavior Rule Specifications

We propose an adaptive specification based intrusion detection system (IDS) for detecting malicious unmanned air vehicles (UAVs) in an airborne system in which continuity of operation is of the utmost importance. An IDS audits UAVs in a distributed system to determine if the UAVs are functioning normally or are operating under malicious attacks. We investigate the impact of reckless, random and opportunistic attacker behaviors (modes which many historical cyber attacks have used) on the effectiveness of our behavior rule-based UAV IDS (BRUIDS) which bases its audit on behavior rules to quickly assess the survivability of the UAV facing malicious attacks.Through a comparative analysis with the multi-agent system clustering model (MAS/ACCM), we demonstrate a high detection accuracy of BRUIDS for compliant performance. By adjusting the detection strength, BRUIDS can effectively trade higher false positives for lower false negatives to cope with more sophisticated random and opportunistic attackers to support ultra safe and secure UAV applications

Data Randomization and Cluster-Based Partitioning for Botnet Intrusion Detection

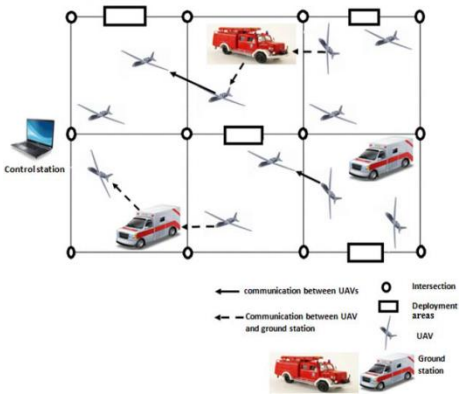
Botnets, which consist of remotely controlled compromised machines called bots, provide a distributed platform for several threats against cyber world entities and enterprises. Intrusion detection system (IDS) provides an efficient countermeasure against botnets. It continually monitors and analyzes network traffic for potential vulnerabilities and possible existence of active attacks. A payload-inspection-based IDS (PI-IDS) identifies active intrusion attempts by inspecting transmission control protocol and user datagram protocol packet's payload and comparing it with previously seen attacks signatures. However, the PI-IDS abilities to detect intrusions might be incapacitated by packet encryption. Traffic-based IDS (T-IDS) alleviates the shortcomings of PI-IDS, as it does not inspect packet payload; however, it analyzes packet header to identify intrusions. As the network's traffic grows rapidly, not only the detection-rate is critical, but also the efficiency and the scalability of IDS become more significant. In this paper, we propose a state of- the-art T-IDS built on a novel randomized data partitioned learning model (RDPLM), relying on a compact network feature set and feature selection techniques, simplified sub spacing and a multiple randomized meta-learning technique. The proposed model has achieved 99.984% accuracy and 21.38 s training time on a well-known benchmark botnet dataset. Experiment results demonstrate that the proposed methodology outperforms other well-known machine-learning models used in the same detection task, namely, sequential minimal optimization, deep neural network, C4.5, reduced error pruning tree, and random Tree.

Network Anomaly Detection: Methods, Systems and Tools

Network anomaly detection is an important and dynamic research area. Many network intrusion detection methods and systems (NIDS) have been proposed in the literature. In this paper, we provide a structured and comprehensive overview of various facets of network anomaly detection so that a researcher can become quickly familiar with every aspect of network anomaly detection. We present attacks normally encountered by network intrusion detection systems. We categorize existing network

anomaly detection methods and systems based on the underlying computational techniques used. Within this framework, we briefly describe and compare a large number of network anomaly detection methods and systems. In addition, we also discuss tools that can be used by network defenders and datasets that researchers in network anomaly detection can use. We also highlight research directions in network anomaly detection.

5. ARCHITECTUREDIAGRAM



ALGORITHM

- **Greedy Perimeter Stateless Routing**

Greedy Perimeter Stateless Routing protocol for wireless datagram networks uses the positions of routers and a packet's destination to make packet forwarding decisions. GPSR makes greedy forwarding decisions using only information about a router's immediate neighbors in the network topology. When a packet reaches a region where greedy forwarding is impossible, the algorithm recovers by routing around the perimeter of the region. By keeping state only about the local topology, GPSR scales better in per-router state than shortest-path and ad-hoc routing protocols as the number of network destinations increases. Under mobility's frequent topology changes; GPSR can use local topology information to find correct new routes quickly.

- **Dijkstra Shortest Path Algorithm**

The Dijkstra Algorithm finds the shortest path from a source to all destinations in a directed graph (single source shortest path problem). During this process it will also determine a spanning tree for the graph.Finding the shortest path in a network is a commonly encountered problem. For example you want to reach a target in the real world via the shortest path or in a computer network a network package should be efficiently routed through the network.

REFERENCE

[1] E. Yanmaz, R. Kuschnig, and C. Bettstetter, “Channel measurements over 802.11a-based UAV-to-ground links,” in Proc. IEEE Globecom Wi-UAV Workshop, Houston, TX, USA, 2011, pp. 1280-1284.

[2] M.O.Cherif, S.-M.Senouci, and B.Ducourthial, "Efficient data dissemination in cooperative vehicular networks, Wireless Commun. Mobile Comput., vol. 13, no. 12, pp. 1150-1160, 2013.

[3] M. Raya, P. Papadimitratos, I. Aad, D. Jungels, and J.-P. Hubaux, "Eviction of misbehaving and faulty nodes in vehicular networks," IEEE J. Sel. Areas Commun., vol. 25, no. 8, pp. 1557-1568, Oct. 2007.

[4] S. Ruj, M. A. Cavenaghi, Z. Huang, A. Nayak, and I. Stojmenovic,"On data-centric misbehavior detection in VANETs," in Proc. IEEE Veh. Technol. Conf. (VTC Fall), San Francisco, CA, USA, 2011, pp. 1-5.

[5] H. Sedjelmaci, S. M. Senouci, and M. Feham, "An efficient intrusion

detection framework in cluster-based wireless sensor networks," Security Commun. Netw., vol. 6, no. 10, pp. 1211-1224, 2013.

[6] X. Haijun, P. Fang, W. Ling, and L. Hongwei, "Ad hoc-based feature

selection and support vector machine classifier for intrusion detection,"

in Proc. IEEE Int. Conf. Grey Syst. Intell. Services, Nanjing, China, 2007, pp. 1117-1121.

[7] C. Callegari, S. Vaton, and M. Pagano, "A new statistical method for detecting network anomalies in TCP traffic," Eur. Trans. Telecommun.,vol. 21, no. 7, pp. 575-588, 2010.

[8] A. Mitrokotsa and A. Karygiannis, "Intrusion detection techniques in sensor networks," in Wireless Sensor Network Security (Cryptology and Information Security Series). Amsterdam, The Netherlands: IOS Press, 2008, pp. 251-272.

[9] M. Strohmeier, V. Lenders, and I. Martinovic, "On the security of the automatic dependent surveillance-broadcast protocol," IEEE Commun. Surveys Tuts., vol. 17, no. 2, pp. 1066-1087, 2nd Quart., 2014.

[10]K. D. Wesson, T. E. Humphreys, and B. L. Evans. Can Cryptography Secure Next Generation Air Traffic Surveillance? [Online]. Available
https://radionavlab.ae.utexas.edu/images/stories/files/papers/adsb_for_ submission.pdf