International Journal of Advanced and Innovative Research (2278-844)/

Volume 7 Issue 11

Vampire attacks: Drainin life from wireless AD-HOC sensor Network

[1]Lekhya Meka, [2]M. Manikanta Rao

[1]Research Scholar, [2]Assistant Professor, Department of Computer Science & Engineering

KODADA Institute of Technology & Science For Women, Kodad

Abstract: Ad hoc low-power wireless networks are an exciting research direction in sensing and pervasive computing. Prior security work in this area has focused primarily on denial of communication at the routing or medium access control levels. This paper explores resource depletion attacks at the routing protocol layer, which permanently disable networks by quickly draining nodes' battery power. These "Vampire" attacks are not specific to any specific protocol, but rather rely on the properties of many popular classes of routing protocols. We find that all examined protocols are susceptible to Vampire attacks, which are devastating, difficult to detect, and are easy to carry out using as few as one malicious insider sending only protocol-compliant messages. In the worst case, a single Vampire can increase network-wide energy usage by a factor of ODNÞ, where N in the number of network nodes. We discuss methods to mitigate these types of attacks, including a new proof-of-concept protocol that provably bounds the damage caused by Vampires during the packet forwarding phase.

Index Terms—Denial of service, security, routing, ad hoc networks, sensor networks, wireless networks

1. INTRODUCTION

The objective of our study to propose a randomized multi-path routing algorithm that can overcome the worm holes formed by Compromised-node and denial-of-service attacks. Instead of selecting paths from a pre-computed set of routes, our aim is to compute multiple paths in a randomized way each time an information packet needs to be sent, such that the set of routes taken by various shares of different packets keep changing over time. As a result, a large number of routes can be potentially generated for each source and destination.

Major challenge of dynamic reconfiguration is Quality of Service (QOS) assurance, which is meant to reduce application disruption to the minimum for the system's transformation. However, this problem has not been well studied. This paper investigates the problem for component-based software systems from three points of view. First, the whole spectrum of QOS characteristics is defined. Second, the logical and physical requirements for QOS characteristics are analyzed and solutions to achieve them are proposed. Third, prior work is classified by QOS characteristics and then realized by abstract reconfiguration strategies. On this basis, quantitative evaluation of the QOS assurance abilities of existing work and our own approach is conducted through three steps. First, a proof-of-concept prototype called the reconfigurable component model is implemented to support the representation and testing of the reconfiguration strategies. Second, a reconfiguration benchmark is proposed to expose the whole spectrum of QOS problems. Third, each reconfiguration strategy is tested against the benchmark and the testing results are evaluated. The most important conclusion from our investigation is that the classified QOS characteristics can be fully achieved under some acceptable constraints.

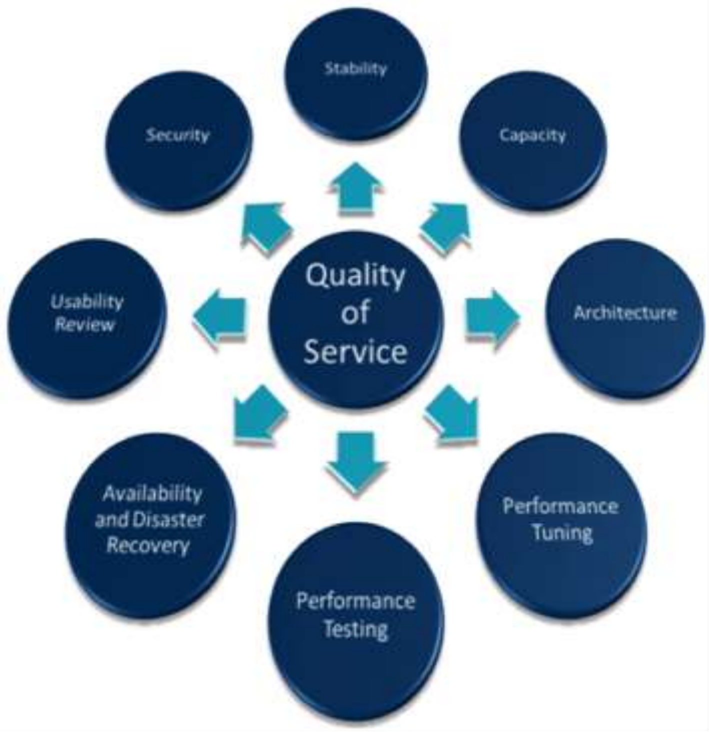

Figure 1.1: Services Provided By Quality Of Service.

Nowadays, number of vehicles is expanding on roads immeasurably. Subsequently road accident and congested road is one of the major developing issues. Therefore, research on enhancing road security and safety application is a subject of concentration. By conveying or communicating through wireless networks, security applications can be used to stay away from such kind of accidents [1].

2. LITERATURE REVIEW

An overview over the various techniques which are used to control congestion are presented in this chapter. There are various other techniques which are used to control congestion present in vehicular ad-hoc networks. These techniques follow the different types of approaches to disseminate data and control congestion. Since Vehicular ad-hoc networks (VANETs) are designed to enable communication between vehicles having infrastructure or without any fixed infrastructures and design for special purpose work for example road safety, data sharing between vehicles, providing entertainment to travelers etc [9]. Hence it is necessary that data dissemination should be easy and congestion should be controlled in the network. The present techniques are describing the diverse methods for energying and congestion control. To overcome the problems of existing technique , the energying based congestion control technique is proposed in this dissertation.

Formal Analysis of a VANET Congestion Control Protocol through Probabilistic Verificationwritten by SavasKonur and Michael Fisher[6]. Vehicular ad hoc networks (VANETs), which are a class of Vehicular ad hoc networks, have recently created a standard method for correspondence among moving vehicles. Since VANETs are imperative to the wellbeing and safety of the vehicles, the people and the infrastructure, a profound analysis of their potential behavior is obviously required. In this paper they give this analysis using formal verification. In particular, they formally examine a particular congestion control protocol for VANETs utilizing a probabilistic model checking procedure, and researching its effectiveness and adequacy.

Congestion Control by Dynamic Sharing of Bandwidth among Vehicles in VANET written by TrishitaGhosh and SulataMitra [7]. The remote access in vehicular environment system is created for upgrading the driving security and comfort of car users. In any case, such framework endures from quality of service degradation for security applications brought on by the direct congestion in scenarios with high vehicle density. The work is a congestion control technique in which vehicular networks are safe from congestion. It supports the correspondence of protected and unprotected messages among vehicles and infrastructure. Every node keeps up a control queue to store the protected messages furthermore, a service queue to store the unsafe messages. The control channel is utilized for the transmission of safe messages and service channel is utilized for the transmission of unprotected messages. Every node figures its own particular priority contingent on the number of waiting messages in control queue and service queue. Every node holds a small amount of control channel and benefit channel powerfully relying on the quantity of holding up messages in its queue. The unprotected messages at a node may likewise be transmitted by utilizing the control channel and provided the control channel is free and service channel is over-burden which helps in reducing loss of unprotected message at a node which in turn decreases the congestion level of a node furthermore improve quality of services. The bandwidth is moreover conveyed among the nodes powerfully relying on their need and priority. The execution of the proposed plan is assessed on the premise of average loss of unsafe message.

Forwarding Methods in Data Dissemination and Routing Protocols for Vehicular Ad Hoc Networks written by Yousef-AwwadDaraghmi and Chih-Wei Yi [8]. Irregular connectivity, sudden changes in network topology and low reception rate are the most vital properties that recognize and distinguish VANET from different sorts of ad-hoc networks. To streamline reliability and time criticality measurements in data communication protocols for VANET, different thoughts are required. In this paper, they show an instructional exercise on techniques (at the network layer), experienced in recent writings, for little and large scale routing protocols, and geocasting (information scattering ,broadcasting and cautioning conveyance) protocols.

Energying-based Algorithm for Connectivity Maintenance in Vehicular Ad-Hoc Networks written by Ahmed Louazani, Sidi Mohammed Senouci, Bendaoud Mohammed Abderrahmane [9]. Among recent technology advances , Vehicular Ad-hoc Networks (VANETs) have drawn the consideration of both scholarly and industry analysts because of their potential applications including driving security, stimulation, crisis applications, and substance sharing. VANET systems are described by their high versatile topology changes. Energying is one of the control plans used to make this global topology less dynamic. It permits the development of dynamic virtual backbone used to sort out the medium access, to support QoS and to rearrange and simplify routing. For the most part, nodes are composed into energy with no less than one energy head (CH) node that is in charge of the coordination undertakings of its energy.

Collision Avoidance System for Safety Vehicular Transportation in VANET written by P.Suresh and M. Ramya [10].A Vehicular Ad Hoc network (VANET) is a rising innovation among the researchers and vehicular industries as of late. The remote impact od collision Avoidance (CA) system sends early message to drivers before they achieve mishap zone out and about. This paper proposed a diagnostic model for warning messages through collision avoidance (CA) system. Utilize the Dichotomized head way model, the Braking model, and Greenberg's logarithmic model to make vehicular mobility traces. The principle concern is to decrease delay while exchange message starting with one vehicle then onto the next vehicle and Utilizing least number of road side units (RSUs).The real concern identified with VANET is congestion control (CC), and quickly changing topology and absence of central coordination. They utilize collision avoidance system for the security transportation and get periodic messages and reduce traffic activity in highway.

Congestion control approach by reducing the number of messages in VANET written by Prabhakar Kumar, Hardip Singh Kataria and TrishitaGhosh [11]. The fundamental substance of this proposed technique for the control of congestion in VANET is exploiting the effectively existing resources of the network and in the meantime keeping the unwanted overheads of nodes and also the connections of network. The control of congestion in the network, for example, vehicular ad-hoc endures an uncommon sort of difficulties. These difficulties are the results of the ecological specificity, for example,often time changing of the topology, expansive measure of varieties in the node density, nature of the correspondence in broadcasting and the confrontational attributes of the neighbor and so on.

Probability Based MAC Channel Congestion Control Mechanism for VANET written by Mark Chih-Wei Hsu and Tien-Yuan Hsieh [12]. A huge issue in VANETs (Vehicular Ad Hoc Systems) is the plan of a successful MAC (Medium Access Control) or broadcast scheme which can encourage the quick and reliable dissemination of basic safety messages to neighboring vehicles if there should arise an occurrence of a surprising occasion. Broadcasting of information, data and control packets is relied upon critical vehicular environment. The vast majority of the broadcasting packet is intended to be conveyed on a given frequency during the control channel (CCH) interval set by the IEEE 1609.4 standard (which gives upgrades to the IEEE 802.11p MAC by supporting multi-channel operation). In this paper, the probability based MAC channel congestion control technique is produced to adapt to fast topology changes, i.e., vehicles entering and leaving the system, and also over-burden circumstances as far as expanded number of vehicles and additionally expanded measure of information activity infused without crumpling.

Adaptive Congestion Control for Transmission of Safety Messages in VANET written by Shruti R. Kolte and Mangala S. Madankar[13]. One of the principle explore research region which has pulled in analysts consideration is congestion control in vehicular ad-hoc networks as it is the key issue which should be tended to. Numerous congestion control algorithms and calculations have been proposed to control congestion issue, still fitting arrangement has not been found. For this reason different algorithms have been proposed in any case, to the beacons which is similarly critical in the vehicular network. In this paper, a versatile congestion control algorithm has been proposed, which is a time slot based mechanism that address beacons and emergency messages. With the assistance of this proposed mechanism and the organizer determination, emergency messages can be conveyed to its planned beneficiaries or intended user immediately and that to without the cost of beacons.

3. PROBLEM IDENTIFICATION

As per observed there are different problem formulation associated which deals with the existing communication protocol. These are the following protocol identification and problems which gives the drawback of previous algorithm.

1. No efficient approach for the prevention of Wormhole attack is given, most of the algorithm work towards the wormhole attach detection only.
2. Routing approach such as DSR and other DSDV are vector driven which make use of existing computed values.
3. No efficient energy based and enhanced algorithm to select an optimized path is investigated which can further be merge in security aspects and provide a unique path for communication.
4. No Approach which make of security algorithm with complex structure to deal with the anomaly and packet security is committed. Thus an efficient security is required.
5. Algorithm with efficient packet delivery along with maximum security is nowhere introduced.
6. Previous algorithm exhibit low security with low throughput and also perform with high end to end delay.

Thus these are the problem issues arise in previous techniques which still need to overcome and solve in the further delivery.

4. PROPOSED METHODOLOGY

A new technique is required which resolves all the routing related issues in existing techniques. A security based technique is presented which provides an enhance mechanism to route packet from source to the destination. In this technique a one hop energizing for all the nodes is conducted. Energy is formed in a manner, each node having one link to the other node to transmit data packet. That reduces the time taken to route packet from source to the destination node. Because it takes small span of time to select optimized route to deliver packet from source to the destination.

Proposed Algorithm Pseudo Code

Inputs: Nodes, Input packet, Key, Security parameter, AODV protocol.

Output: Packet transfer, secure packet, optimal route, parameter computation which is PDR, delay and throughput.

Steps:

```
Begin- foreach(Packet i-n)
{
Algorithm initialized();
Key generation ECC();
AODV setup();
findingOptimalHead();
Energyroute selection ();
Return efficient path ();
Security packet transmission();
}
Compute PDR();
Compute End to End Delay();
Compute throughput ();
Return parameter ();
Exit;
End;
```

In computer network, open-source event-driven simulator is invented especially for research called as NS2. Considering its establishment in 1989, NS2 possess continuously won incredible attention from industry, academia, and government. NS2 contains of modules for numerous network additives including routing, transport layer protocol, software, etc. to analyze network performance, researchers can easily use scripting language to configure a network, and perceive consequences generated by way of NS2. NS2 is emerged as the most commonly used open supply network simulator, and one of the maximum extensively used network simulators. Maximum research desires simulation modules that are beyond the scope of the integrated NS2 modules.

5. RESULTS

The aim of these simulations is to analyze the AODV protocol by comparing it with other protocols with security constraint. The following table shows that the important parameters-

(a)Throughput: A throughput of the network is the average rate at which message is successfully delivered between a receiver and sender. It is also referred to as the ratio of the sum of data packet received from its sender to the time the last packet reaches its destination. **Throughput=(Total No.of Successful Packets Received in Bits)/(Total Simulation Time in Sec)**

(b)End To End Delay: The average end to end delay defined as the time taken in delivery of data packets from the source node to the destination node. To calculate the average end-to-end delay, add delay of each successful data packet delivery and divide that sum by the number of successfully received data packets **Average End to End Delay=(∑(Received Time-Sent Time))/(Total Data Packet Received)**

(c)Packet Delivery Ratio: The Packet delivery ratio defined as the delivery of data packets from the source node to the destination node. To calculate the PDR, **Packet delivery ratio=(∑(Total Packet Received))/(Total Data Packet Sent)**

STATISTICAL ANALYSIS: A measurable analysis of the outcomes is done in this section. These sections say about the computed parameter using both the algorithm and their values statically and further are graphically. To analysis of original VANET wormhole attack detection using effective routing, heuristic based approach and VANET efficient path with security algorithm Network Simulator (NS2) was used. The simulate are run for existing AODV and under same environment it will again be run for AODV-SEC or Modified AODV to see the comparison of performance on differences against Average Delay, Packet Delivery Ratio (PDR) and Throughput. The Modified AODV is simulated using with following scenarios given in table 1.1.

Average Delay Vs Speed: Because of multiple path features in modified AODV-ENC packets need not to wait for long.

Table 1.1: Average Delay Vs Speed

Speed	**AODV**	**AODV-ENC**
0	**43.73**	**35.12**
1	**40.67**	**37.87**
5	**73.46**	**71.76**

10	**99.16**	**95.15**
15	**119.12**	**105.12**
20	**126.59**	**125.45**

In the table 1.1 above a simulation analysis in between the existing VANET algorithm and proposed protocol architecture which is using enhance security model. Further average delay is computed on enhancing different speed of node in between the network computation.

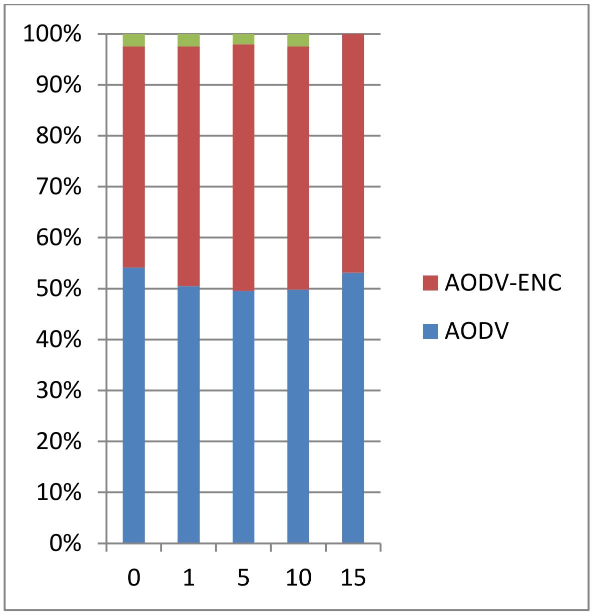

Figure 1.2: Comparison Among Values Of AODV and AODV-ENC.

5. CONCLUSION

VANET is an important part of mobile adhoc network. Today IOT and different communication is taking over the advantage and its future of communication where the all required component is going to connect with each other and help in delivery efficient services. Different approaches in order to communicate and challenges arise is described in previous system. A special type of attack which is focused on our dissertation and on which work is preceded. Wormhole attack prevention is the main objective of our work. This type of attack creates a unique path which communicates in between the available data packet transfer without using efficient path. Thus an enhancement in routing path delivery algorithm is required.

Our thesis makes use of efficient encryption approach over the packet delivery before it initiate to the network. Elliptic curve model for the security over the data packet transfer such that the packet which are being transferred are driven in given route and not be distracted. Also the efficiency is derived from the heuristic integration which gives packet transfer in particular decided path. Thus the wormhole attack is avoided using the algorithm approach followed by us. It increases the network efficiency while comparing with existing AODV protocol without extra leverage protocol heuristic and security approach. To show the efficiency of our approach proposed and existing protocol implemented using NS2 simulator and performed with parameter PDR, end to end delay and throughput. Computed parameter and their values show the effectiveness of our approach.

A better communication protocol with enhancement in security along with heuristic is proposed which compute efficiency towards packet transfer and also it helps in avoid wormhole attack.

REFERNCES

[1]. Mario Gerla, Eun-Kyu Lee, Giovanni Pau, and Uichin Lee," Internet of Vehicles: From Intelligent Grid to Autonomous Cars and Vehicular Clouds",IEEE 2014

[2]. T. Taleb, E. Sakhaee, A. Jamalipour, K. Hashimoto, N. Kato, and Y. Nemoto, "A stable routing protocol to support its services in vanet networks" IEEE Transactions onVehicular

Technology, vol. 56, no. 6, pp. 3337–3347, November 2007.

[3]. Manvi, S.S., Kakkasageri, M.S., Mahapurush, C.V., “Performance Analysis of AODV, DSR, and Swarm Intelligence Routing Protocols In Vehicular Ad hoc Network Environment” In International conference on future Computer and Communication., pp. 21-25, April. 2009.

[4]. Bernsen,J. Manivannan,D.,“Routing Protocols for Vehicular Ad HocNetworks That Ensure Quality of Service” In the fourth international confernce on Wireless and Mobile Communications., pp.1-6, Aug. 2008.

[5]. Wex p Breuer,J. Held,A. Leinmuller,T. Delgrossi,L.,“Trust Issues for Vehicular Ad Hoc Networks” IEEE,VTC Spring 2008., pp. 2800-2804, May.2008.

[6]. David B. Johnson, David A. Maltz, and Josh Broch, “DSR: The Dynamic Source Routing Protocol for Multi-Hop WirelessAd Hoc Networks”, in Ad Hoc Networking, Editor: Charles E.Perkins, Chapter 5, pp. 139-172,Addison-Wesley, 2001

[7]. Ding y Wang C, Xiao L “A static-node assisted adaptive routing protocol in vehicular networks”

[8]. Francesco Malandrino, Francesco Malandrino “In Proceedings of the Fourth ACM international Workshop on Vehicular Ad Hoc Networks VANET”, pp 59–68, 2007

[9]. Kumar, L. Shi, S. Gil, N. Ahmed, D. Katabi, and Daniela, “CarSpeak: A Content-Centric Network for Autonomous Driving,” in ACM SIGCOMM, Aug. 2012

[10]. .J. C. Zhao, G “VADD: Vehicle-Assisted Data Delivery in Vehicular Ad Hoc Networks” INFOCOM 2006. 25th IEEE International Conference on Computer Communications. Proceedings, pp. 1 - 12, April 2006.

[11]. A. Zanella, N. Bui, A. Castellani, L. Vangelista, and M. Zorzi, “Internet of Things for smart cities,” IEEE Internet Things J., vol. 1, no. 1, pp. 22–32, Feb. 2014

[12]. Mohammad Ali Salahuddin, Member, IEEE, Ala Al-Fuqaha, Senior Member, IEEE, and Mohsen Guizani, Fellow, IEEE,” Software-Defined Networking for RSU Clouds in Support of the Internet of Vehicles”,2015.

[13]. Dr.AndrawsSwidana , Eng. HaythamBaniAbdelghanya*, Dr.RamziSaifana , Dr.ZeljkoZilic,” Mobility and Direction Aware Ad-hoc On Demand Distance Vector routing protocol”, Elsevier 2016.