VANET-Inter Military Tanks Communication using Wireless Sensor Networks with Collision Prevention and Grenades Availability Protection

[1]Sachin Jindal, [2]Dinesh Kumar
[1]Dept. of CSE, Gaini Zail Singh Punjab Technical University Campus, Bathinda, Punjab, India
[2]Gaini Zail Singh Punjab Technical University Campus Bathinda, Punjab, India

Abstract
The review paper is proposed to implement VANET in military applications at war time. VANET is an ad hoc network which consists of vehicular ad hoc network oriented military tanks. This type of VANET has different challenges if we compare with the normal tank war. To understand the problem the VANET is to be simulated using java socket programming in which various issues are described mainly consists of neighbor tank position updates, collision prevention between tanks and also the main security issue of availability of grenades in the tank. If any tank gets out of stock of grenades then automatically updates to be sent to the neighbor tanks so that the protection cover can be provided.
This review paper also discusses different number of scenarios of VANET which we implement in our simulation. In our simulation we use to implement VANET using different vehicles which communicate to the neighbor (WSN) wireless sensor network placed at distance apart. The vehicles are taken as tanks which are used for war. The neighbor updates are send via WSN which are placed under earth at war zone.

Keywords
VANET, Ad-Hoc Network, Wireless Sensor Networks, Military Tanks Inter Communication, Simulation

I. Introduction

Vehicular Ad Hoc network got outstanding success as well as tremendous attention due to its self maintenance and self configuration properties of behavior. At early stage mostly people focused on its friendly and cooperative environment and due to this way many different problems came in being; security is one of the primary concerns in order to provide communication between different nodes in a Vehicular ad hoc network war environment. Due to different characteristics of Vehicular ad hoc network neighbor updates is an active research topic in wireless path, which is also a non-trivial challenge to communication design. There are different types of challenges in
Challenges for VANET are given below.

- Open network architecture
- Shared wireless medium
- Stringent resource constraint
- Highly dynamic network topology
- Resources availability

It is also true that the solutions to the wired networks do not workable to Vehicular ad hoc network domain.
WSN has different challenges with respect to VANET due to some of the following reasons:

1. The wireless network especially liable to attacks because of active eavesdropping to passive interfering.
2. Due to lack of Trusted Third Party adds, it is very difficult to deploy or implement security mechanisms.
3. Mostly Vehicular devices have limited computation capability and power consumption functionalities which are more vulnerable to Denial of Service attacks. It is also incapable to run heavy security algorithms which need high computations like public key algorithms.
4. Due to WSN's properties like infrastructure less and self-organizing, there are more chances for trusted node to be compromised and launch attacks on networks. In other words we need to cover up from both insider and outsider attacks in WSN, in which insider attacks are more difficult to deal with.

II. Aims and Objectives

VANET is a type of multi-hop network, infrastructure less and the most important self-organizing. Due to its wireless and distributed nature there is a great challenge for system updates to the neighbor nodes and how they can access to each other and importantly how can they guess their position relative to the target. So VANET are aimed to combine with WSN in which the client server architecture is deployed where client is VANET and server is WSN is working respectively.
One of the main characteristic of VANET's with respect to security design point of view is the lack of clear line defense. In case of wired networks we have dedicated routers; which perform routing functionalities for devices but in case of Vehicular ad hoc network are concerned each Vehicular node acts as a router and forward packets for other nodes. It is also true that the wireless channel is accessible to both network users as well as to attackers. There is no well defined rule or place where traffic from different nodes should be monitored or access control mechanisms can be enforced. Due to this way there is no any defense line that separates inside network from the outside network. Due to this way the existing ad hoc routing protocols, like Dynamic Source Routing (DSR) and Ad Hoc On Demand Distance Vector (AODV) , and wireless MAC protocols, such as 802.11, typically assumed to be trusted. As a result, an attacker can become a router and disrupt network operations. To setup communication between the moving vehicles like tanks are in our case there must be some neighbor wireless sensor networks who capture the information time to time from the vehicles and sends updates to the other vehicles in the same zone.

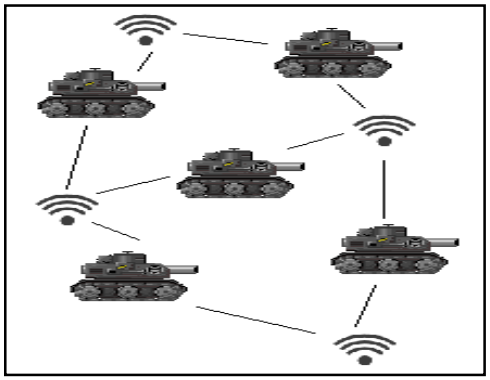

Fig. 1: Vehicular Inter Communication Using Wireless Sensor Network

As shown in the fig. 1 in which Tanks inter communication taking place using WSN. Tank can send the update to the wireless network and this network keeps track of all the tanks information and updates to the neighbor wireless sensor nodes. Further for any kind of neighbor tank information can be sent to other tanks.
There are mainly three main issues are addressed in this paper.

1. Secure communication between the VANET nodes.
2. Collision detection and prevention between the VANET nodes.
3. Resources update and availability between the VANET nodes.

Among all these security services, availability is probably the most important and complex issue in military war VANET because it is the bootstrap of the whole security system. This become very crucial when grenades for one particular or more tanks get empty then there is other way available to inform other neighbors in the war zone about to cover and protect the tank. So the protocol can be designed with the help of wireless sensor network as a server who keep updated and informed about each other distance, grenades etc status.

III. Research Goals

In this paper we mainly focus on the implementation of VANET with WSN and security threats mainly covers availability and challenges in VANET. There are two main parts of our paper, in the first part we have discussed different security aspects and how these issues to be resolved? In the second part of the thesis there will be an implementation of VANET using JAVA VANET/WSN simulator; first we will develop VANET with different routing protocols and implement the inter communication setup between different VANET nodes. To do this task we have to implement the wireless sensor network in the neighbors zone of each moving tank and has to design the protocol for vehicles updates that is required to update neighbors information.
Secondly we will develop a protocol in which the moving tanks can prevent itself w. r. t. two different harms.

1. Collision between the tanks.
2. Grenades availability information update so to protect tanks with no grenades left.

In general there are following research questions which we will discuss in our paper:
RQ1: How tank moves and changes the speed along with distance covered and updates to WSN nearby to the network?
RQ2: Wireless sensor which receives latest updates from various tanks and verifies the speed and distance covered and sends back the signals to the tanks so collision can be prevented so how this information can send to the moving vehicles?
RQ3: Implementation of VANET and what are the challenges for VANET to keep updated and protected when goes empty with grenades by other neighbor tanks.
RQ4: How can we deal with security threat of availability of grenades to tank within VANET?

IV. Research Methodology

This research requires and an incremental approach to design the whole system with step by step implementation of different requirements. As the requirements are mentioned below to implement the VANET military tanks system using WSN.

1. Inter communication for VANET
2. Intra communication for VANET and WSN
3. Neighbors updates
4. Distance updates
5. Collision detection and prevention
6. Grenades stock update for all tanks
7. Protection cover for tanks with no grenades left.

The whole system can be designed using simulation concept

V. Simulation

The simulator that will be required to implement this research work will be developed in some language which supports socket programming like java is one example which will be exclusively designed and worked for VANET.
In this simulator the model will be implemented in two different parts where one part will refer to the VANET and other part will be WSN.
The server node will keep focus on the client nodes activities their movements, attacks and security issues if any faced by the nodes. And corresponding the old protocols that worked previously to prevent different attacks will be implemented along with the newer modified protocols that will be designed in this research work also get implemented on the same simulator network. Thus the calculations with respect to delay, throughput, resistance etc parameters will be calculated by the VANET for the client nodes and the comparative study will be taken out by the simulator.

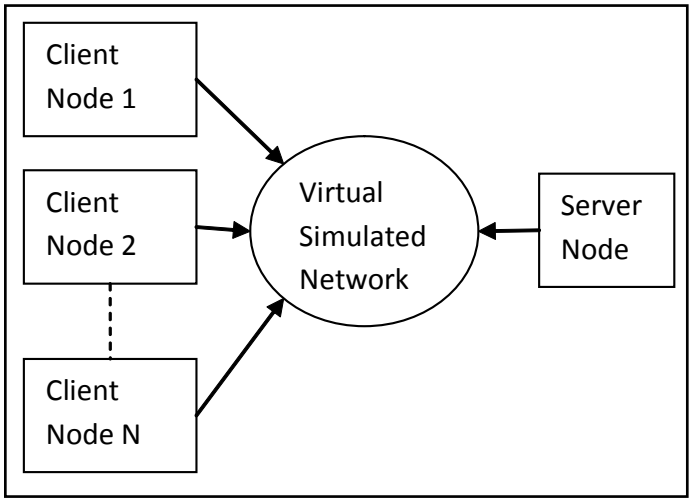

Fig. 2: Simulated Design of VANET using WSN

The design of network is shown above can be built using java language with implementation of the network using Socket Programming in which the sockets can bind together over the network and all the nodes in a network behave like a moving vehicle and address along with timely reporting to the server node.

VI. Conclusion

VANET are the kind of networks becoming very popular and useable now a days. As we studied ad hoc network are the kind of temporary networks which can be established anywhere between two and more communication devices without standard protocols implementations. Out of these VANET are one type of ad hoc network called Vehicular Ad hoc Network which get worked between the two or more moving vehicles. As it is ad hoc network so must be hacking prone network as there are no standard implementations of protocols are there. So we have to address all those main issues and to put an effort to reduce and even overcome all those effects which breaks the security constraints in the network. So aim of this research is to figure out security issues includes inter communication for neighbor updates, distance updates, grenades updates which arise in VANET as

well as to overcome the issue of resource availability along with implementation of VANET over a simulated environment which will be based on JAVA Socket Programming.

Reference

[1] Sandeep Tayal, Malay Ranjan Tripathy,"VANET-Challenges in selection of Vehicular Mobility Model", International conference on Advance Computing & Communication Technology, 2012.

[2] Ghassan Samara,"Security Issues and Challenges of Vehicular Ad Hoc Networks (VANET)", School of Computer Science, Universiti Sains, Malaysia.

[3] Rongyan Xia, ChenYe, Dongdong Zhang,"Vehicle to Vehicle and Roadside Sensor communication for Intelligent Navigation", Shanghai 200092, China

[4] Vineetha Parachuri,"Inter-Vehicular Communication: Security and Reliability Issues", RV college of engineering, Banglore, India.

[5] Patrice Seuwou, Dilip Patel, Dave Protheore, George Ubakanma,"Effective Security as an ill-defined Problem in Vehicular Ad Hoc Networks (VANETs)", Department of Infomatics, London South Bank University, London.

[6] Ikecukwu K. Azogu, Michael T. Ferreira, Hong Liu,"A Security Metric for VANET Content Delivery", Department of Electrical and Computer Engineering University of Massachusetts Dartmouth, USA

[7] Hua Qin, Zi Li, Yanfei Wang,Xuejia Lu, Wensheng Zhang "An Integrated Network of Roadside Sensors and Vehicles for Driving Safety: Conecpt, Design and Experiments", Department of Computer Science, Iowa State University, USA

[8] Jinat Rehana,"Security of Wireless Sensor Networks", Helsinki University of Technology.

Sachin Jindal received his B.Tech. degree in CSE Stream from Baba Farid College of Engineering & Technology, Deon, Bathinda, in 2012, the M.Tech. degree in CSE from Gaini Zail Singh Punjab Technical University Campus, Bathinda, in 2014. His research interests include Vehicular Ad-Hoc Networks and Wireless Sensor Networks.

Er. Dinesh Kumar is currently working as Assistant Professor in Deptt.of Computer Science and Engineering. His Areas of research Include Computer Networking.He has Attented various International and National Conferences.