A Secured Communication Technique for Unmanned Vehicles using VANET

Thangakumar Jeyaprakash
Department of Computerscience and Engineering
Hindustan University, India
tkumar@hindustanuniv.ac.in

Rajeswari Mukesh
Department of Computerscience and Engineering
Hindustan University, India
rajeswarim@hindustanuniv.ac.in

***Abstract* — Unmanned Ground Vehicles (UGV) are playing a vital role in Military Services. The main abstract of this project is proposed for provide a Tactical information Management system for Unmanned Ground Vehicles using Vehicular Ad-hoc Networks [1] (VANET). VANET is a perfect option for vehicle to vehicle communication to share the Information with each other. An Information Control Unit will be attached in-built with all unmanned ground vehicles to share the information. An Information Control unit consists of front and rear Radar (Radio Detection and Ranging), Event Data Recorder, Global positioning system (GPS), Sensor, and a communication system. When a failure detected in an Unmanned Ground vehicle due to the enemy attack, the tactical information will be shared with the help of proposed encryption technique with the neighboured UGVs among the VANET about the status of failed UGV. The damaged UGV will be replaced immediately with the neighbour to fill up the gap using the Tactical information shared using the WAVE (Wireless Application for Vehicle Environment) SMS protocol. This information is used to avoid collision also during fog.**

Keywords - Unmanned Vehicles, Vehicular Adhoc Networks, Radio Detection and Ranging.

A shorter version of this paper was presented at ISMS2013, 29-31 January, Bangkok, ISBN 978-0-7695-4963-7, pp 472-475

I. INTRODUCTION

Vehicular Adhoc Networks plays a vital role for any Road transportation system. Once the VANET is formed, three types of communication are possible. 1. Vehicle to Vehicle communication (VV) 2. Vehicle to infrastructure Communication (VI). 3. Infrastructure to Vehicle Communication. (IV). The infrastructure unit is otherwise called as the Road side Station (RSS). Each vehicle is inbuilt with the Onboard Unit (OBU).Each vehicle will broadcast messages to the neighbor vehicles with the help of OBU[12]. The messages contain the direction, location, speed, time and a warning message too during the critical situation. The Message will be a traffic related, it will be transmitted in single hop and if it is emergency related, the message will be transmitted to n number of vehicles through multi hop transmission. These messages will helps in avoiding the possible damage or help the driver to decide for the better route. The message broadcasted is subject to authenticity, Integrity and Privacy. IEEE 802.11p is a standard for Wireless Access Vehicular Environment for the communication of nodes in the Vehicular Adhoc Networks. The operating frequency of short range communication of WAVE is 5.85 – 5.925 GHz [11]. This frequency will provide communication over 5 – 10 km.

Components of VANET:

The components used in a vehicle are 1. Event Data Recorder 2. Unique Identification number 3. Global Positioning system (GPS) 4.Sensors to detect Obstacles 5.Special devices used to provide Communication of Vehicular adhoc networks. Most Authors may handle communication of the messages with the digital signature with the public key certificate issued by the certification authority.

Characteristics of VANET:

Each Network will exhibit communication delay due to the change in Environmental conditions, the excess speed of other vehicles etc. The VANET should have high authenticity, scalability and privacy. The driver should trust the message to decide the route in emergency broadcasted from other vehicle. It should not be the fake message.

Challenges of VANET:

High node mobility, Privacy and security, No delay can exist due to the change in environmental conditions, Radio channels which will degrade the strength and quality of signals. Routing in VANET is one of the important challenges of VANET. VANET routing can be done by two options. 1. Proactive mode 2. Reactive mode. Proactive mode routing broadcasts or receives messages periodically and the Reactive mode broadcasts or receives message only any incident happens. In proactive mode, an accident in a parked vehicle can be easily identified for further liabilities by using its sensors data information stored in the onboard unit. Reactive protocols such as AODV (Adhoc on demand distance vector routing protocol) and Distance source routing (DSR) also can be used for VANET.

Security Threats in VANET:

Security is the most important aspect in the communication of VANET. Denial of Service (DOS) attack[12] and sending of false warnings will be happening

possibly by the attackers. Injecting false, modified and repeated messages will leads to exploit the VANET in different situations. An attacker is an entity who wants to spread the false information to other vehicles to make the VANET functioning improperly. Possibly two types of attackers are present. 1. External attackers 2. Internal attackers. External attackers are the nodes outside the network try to get unauthorized access to inject false information to make the network stop functioning properly. Internal attackers are the nodes present inside the network try to spread the false information. These misbehaving nodes are known as malicious nodes which introduce invalid data into the network to produce communication failures. These failure leads to communication delay. So, an Effective cryptographic mechanism is used to provide security to achieve the trustworthy communication of VANET. Either, It is internal or external attackers, the attacker is used to extract the data such as time, speed, location from the attacked vehicle and try to collect the private information from the attacked node.

Encryption technique for the proposed Architecture:

The main cryptographic requirements for the secret communication of unmanned vehicles using Vehicular adhoc networks are 1. Availability: The network should be available all the time to communicate with other vehicle or to send and receive messages. 2. Integrity: The secret information sent by the vehicle should not be corrupted 3. Confidentiality: High Secrecy must be provided to the packets sent over the network. 4. Authenticity: The authorized node only should receive the message for the authorized sender node, that is, more authentications must be provided between the networks..The Communication society establishment of Canada approves cryptographic algorithms for the protection of sensitive information and for the electronic authorization. The approved key establishment algorithms are RSA (Rivest, Shamir, Adleman) algorithms, Diffie-Hellman Key exchange, and Elliptic curve cryptography algorithm. So, for the proposed architecture, The mentioned above three algorithms are used to establish a shared secret key with the key derivation function to maintain the confidentiality, integrity and authenticity. The Tamper – Proof two dimensional Algorithm array tables for m, n algorithms is given as follows to choose the encryption algorithm randomly during the communication between the tanks

	0	1	2	3.....	.....n
0	0,0	0,1	0,2	0,3	0,n
1	1,0	1,1	1,2	1,3	1,n
2	2,0	2,1	2,2	2,3	2,n
3	3,0	3,1	3,2	3,3	3,n
m	m,0	m,1	m,2	m,3	m,n

Figure 1: Two Dimensional Algorithm Array table

The values m,n are the number of algorithm can be used in the algorithm array table. The Tamper – Proof two dimensional Algorithm array tables for 3X3 array algorithms is given as follows to choose the encryption algorithm randomly during the communication between the tanks.

	1	1	2
0	0,0	0,1	0,2
1	1,0	1,1	1,2
2	2,0	2,1	2,2
0 –Rivest Shamir Adleman Alg 1 – Diffee –Hellman Key Exchange 2 - Elliptic Curve Cryptography (ECC)			

Figure 2: 3X3 Algorithm array table

The message contains the secret data will be encrypted with the random array selected from the algorithm array table. For example, If (0,2) is selected, The message will be encrypted by Rivest Shamir adleman algorithm to get the cipher text and the same will be encrypted by Elliptic Curve Cryptography algorithm.

Then format of the message is given as follows

Cipher text C= {Ts; Td; K; D; E (0, 2) M}

Plain Text M= {Ts; Td; K; D; D (0, 2) C}

Ts- Source Tank
Td – Destination Tank
K- Public key
D- Secret Data
(0, 2) – RSA, ECC
E (0, 2) – Random Encryption algorithm to encrypt the message

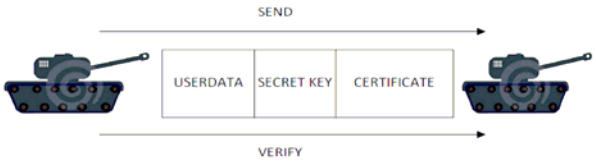

Figure 3: Message sharing between tanks

In figure 3, the secret communication will be shared between the two tanks with the help of effective encryption technique to protect the vehicular adhoc networks from the attackers trying to stop the networks functioning properly. This encryption technique will maintain confidentiality and integrity in networks.

II. Related Works

Enormous amount of Research activities are going on Vehicle Adhoc Networks (VANET) in both National and International countries. Some of the Literature surveys were mentioned below. Blum states[1] that the constraints on vehicle movements, varying driver behaviour, and high mobility cause rapid topology changes, frequent fragmentation of the network, a small effective network diameter, and limited utility from network redundancy. These changes have implications for the IVC architecture at the physical, link, network, and application layers. Rapid changes in the Inter Vehicle Communication (IVC) network topology are difficult to manage. Unlike the redundancy in other MANETs, the redundancy in IVC networks are severely limited both in time and in function. The IVC network has an even smaller effective network diameter under source-generated routing.

H.L. Song states the device is embedded into a cellular phone installed in a vehicle. When this vehicle is travelling through a cellular territory [7], the device receives those signals and calculates the attenuation of those signals to locate the current vehicle position.

Lichtenegger [5] suggests an approach to utilize location information for instance, obtained using the global positioning system) to improve performance of routing protocols for ad hoc networks. DIRICOM Project: "Intelligent Design of Wireless Communication Networks "It is financed by the Spanish regional Ministry for Innovation, Science and Business. The aim of this project is to tackle wireless networks design problems using intelligent techniques.

III. Implementation and Research

In this paper, we proposed that, When the Radar is detecting an Unmanned Ground Vehicle (UGV) by sending and receiving the reflection pulse from the UGV, the tactical information can be shared between the vehicles. Each vehicle will be monitoring by the neighbour nodes. The Scientific importance of the project are analyzing the performance of radar in ranging and detecting the neighbour vehicle, computation of GPS [5] and Communication system with the radar output will be displayed in the Network Display Unit. IEEE WIMAX 802.16 a will be used for setting up the Vehicular Adhoc Network (VANET setup). The scientific Research will be developed to replace the fault Unmanned ground vehicle immediately using the tactical information shared with each other to attack the enemies without leaving any gap between the Unmanned ground vehicles. In figure 4, When the Vehicular adhoc network formed, each node will be monitoring by the neighbour nodes. Each node will be communicating with each other with the help of front radar and the rear radar. Each nodes will be detecting the target by sending and receiving the radio pulse at the rate of 300,000 m/sec. The Global positioning system [6] and the Sensor [8] information will be sending to the computing platform with the radar information. The Event data recorder will record the information such as Fog information to avoid collision during night time, fire control information of the UGV, current performance status of an unmanned vehicle, environmental condition etc.

The Sensor is used to detect the fire control information, fog information, and current status of that particular node.

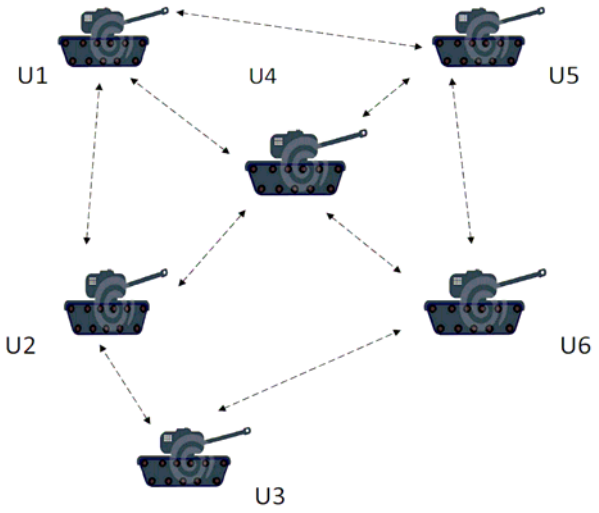

Figure 4: Formation of Vehicular Adhoc network for Unmanned Ground Vehicles

The well equipped Global positioning system is used to navigate the position of the Unmanned Ground vehicle. This information will be sending to the Computing Platform to find the final output of Information Control Unit.

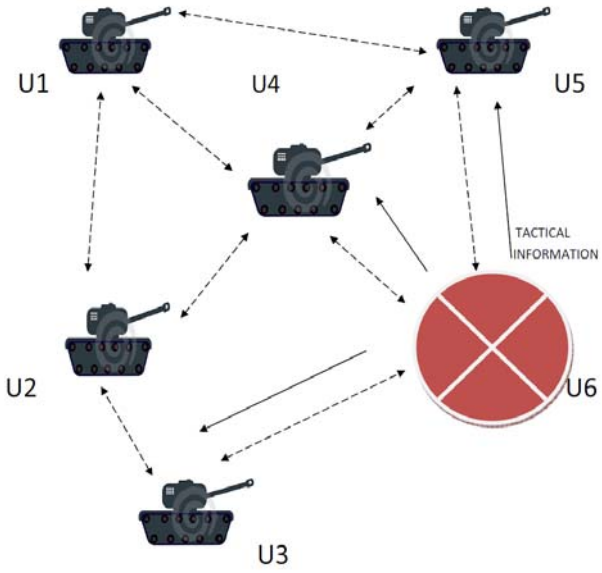

Figure 5: Sharing of Tactical Information from Damaged UGV

In Fig 5, When an Unmanned ground vehicle is attacked by the enemies, the encrypted information will be shared within the neighbour nodes. Immediately, the damaged vehicle gap will be replaced by the nearest node to avoid lagging and attacking the enemies without interference.

Nodes	Monitoring Neighbor nodes
U1	U2,U4,U5
U2	U1,U4,U3
U3	U2,U4,U6
U4	U1,U2,U3,U5,U6
U5	U1,U4,U6
U6	U3,U4,U5

Table 1: Neighbour nodes table

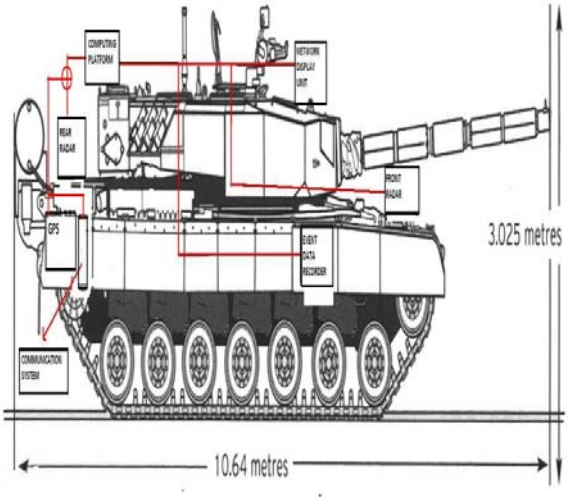

Figure 5: Tank with information Control Unit

In table 1, The U1 vehicle is monitoring by the UGVs U2, U4, U5. The U2 vehicle is monitoring by the UGVs U1, U4, U3 and so on. This table will be displayed in the network display unit involved in the Information control unit. Not only the nodes information, includes Fog information to avoid collision during night time, fire control information of the UGV, current performance status of an unmanned vehicle, environmental condition etc. The information will be shared using the WAVE wireless application for vehicle enhancements protocol using IEEE 802.11a standards.

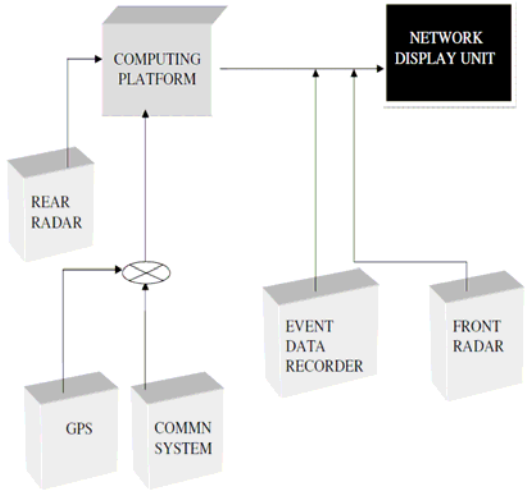

Figure 6: Block Diagram of Information Control Unit

In Figure 6, The GPS and radar information will be computed and send to Network display unit with the EDR data to share the tactical information of their vehicle.

IV. Results and Conclusion

This paper presented the tactical information management system for unmanned ground vehicles (UGV) to provide more security and information sharing. The well equipped global positioning system (GPS) with the Radar information, Sensor information will helps the unmanned vehicles from collision during fog, The Event data Recorder will record each and every event visually. So the weather conditions will be clearly recorded by the Event Data Recorder to send the information frequently to network display unit.

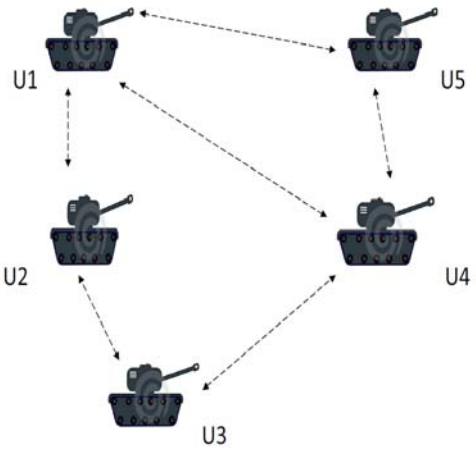

Figure 7: U4 replaced the damaged vehicle U6

The replacement of damaged vehicle by the monitoring neighbour node using the efficient encryption information will helps to fill of the gap of vehicular adhoc networks.

REFERENCES

[1] J. Blum, A. Eskandarian, L. Hoffman, Challenges of inter-vehicle adhoc networks, IEEE Transactions on Intelligent Transportation Systems 5(4) (2004) 347–351.

[2] J. Hubaux, S. Capkun, J. Luo, The security and privacy of smart vehicles, IEEE Security and Privacy Magazine 02 (3)(2004) 49–55.

[3] R. Parker, S. Valaee, Vehicle localization in Vehicular Networks, In Vehicular Technology Conference, 2006. VTC-2006 Fall. 2006 IEEE64th, 2006, pp. 1–5.

[4] Y.-B. Ko, N.H. Vaidya, Location-aided routing (LAR) in mobile adhoc networks, in: Mobile Computing and Networking, 1998, pp. 66–75.

[5] B. Hofmann-Wellenho, H. Lichtenegger, J. Collins, Global Positioning System: Theory and Practice, 4th ed., Springer-Verlag, 1997.

[6] E. Krakiwsky, C. Harris, R. Wong, A kalman filter for integrating dead reckoning, map matching and gps positioning, in: Position Location and Navigation Symposium, 1988. Record. 'Navigation into the 21st Century'. IEEE PLANS'88., IEEE, 1988, pp. 39–46.

[7] H.-L. Song, Automatic vehicle location in cellular communications systems, IEEE Transactions on Vehicular Technology 43 (4) (1994) 902–908.

[8] T. Bass, Intrusion detection systems and multisensor data fusion, Communications of the ACM 43 (4) (2000) 99–105.

[9] G.R. Jagadeesh, T. Srikanthan, X.D. Zhang, A map matching method for gps based real-time vehicle location, Journal of Navigation 57 (2005) 429–440.

[10] R.R. Brooks, S.S. Iyengar, Multi-Sensor Fusion: Fundamentals and Applications with Software, Prentice-Hall, Inc., Upper Saddle River, NJ, USA, 1998.

[11] Claudia Campolo, Alexey Vinel, Antonella Molinaro, and YevgeniKoucheryavy,"Modeling Broadcasting in IEEE 802.11P/Wave Vehicular Networks", IEEE Communications Letters, VOL. 15, NO. 2,PP 199 – 201, February 2011

[12] Security Issues in Vehicular Ad Hoc Networks,P. Caballero-Gil,University of La Laguna,Spain