International Journal of Advanced Trends in Computer Applications
www.ijatca.com

An Individual Trust Management Technique for Mitigating Security Attack in VANET

Er.Karamjit Kaur [1], Er. Kushal Kanwar [2]
[1] CSE (Student), Chandigarh University
karamgrewal09@gmail.com
[2] CSE (AP), Chandigarh University
kushalneo@gmail.com

Abstract: *The key issues of VANETs are routing and security. A secure routing environment provides a better efficiency in terms of data packet delivery and minimizing bit error rate. The information passed through one vehicle for another vehicle must reach on time to prevent the second vehicle from any accident. The message passing system may get affected due to malicious interpretation in the network. In this we establish an efficient routing work which dynamically nodes itself. If it meets any intrusion in the network according to its fitness value designed so that the message passed to the second vehicle reaches on time. We design and implemented a dynamic routing protocol for the successful delivery of the time messages from one vehicle to another and also enhanced the performance of security by implementing a message interchange API system. The parameters which are evaluated given as throughput, error rate, and packet delivery rate.*

Keywords: *VANETs, RSUs, Genetic Algorithm, Trust Management, Security Attacks.*

I. INTRODUCTION

Nowadays transportation structure plays an imperative part in our everyday lives. As of last few decades a novel transportation structure which usually has captivated loads of attention from both industry and academia is VANETs. It is a novel kind of network that is usually anticipated to support a large spectrum of mobile distributed applications applied on vehicles [1]. VANET is a subclass of the MANET. In particularly VANET every single node is a specific category of vehicle otherwise RSU (Road Side Unit) that possibly can move freely within the network range and stay connected. Every single node interconnects through further nodes in a single hop or else multi hop type. VANET make available safe as well as non-safe amenities to the particular drivers [2]. VANET involves short-range radios which are usually installed in specific vehicles, Road Side Units (RSUs) as well as principal consultants which are responsible for identity registration and management. Communiqué in VANET is possibly done by Vehicle to Vehicle (V-V) in addition to Vehicle to Infrastructure (V-I) [3]. However, it is critical for VANET to guard against misuse events, the global association intended for VANET security structural design need to be prudently premeditated for specifically when it is a worldwide executed VANET. The safekeeping of VANETs is utmost acute issues for the reason that their data transmission is propagated in open access (wireless) environments. It is essential that all communicated information which would not be injected or else transformed via users who have malicious goals [4]. In attack the attacker advertise itself as it knows the most recent route towards destination and when the source select the route through it then the node drops the packets hence degrades the network performance. This paper presents an algorithm to maintain trust as an indicator for their genuine behavior.

2. SECURITYs IN VANET

In current years the worry over the security of VANET has been extensively discuss and popularized. The conversation has, however, characteristically involved only static and wired networking while the movable or ad-hoc networking issues have not been handled extensively [5]. The appearance of such new networking approach sets new challenges even for the essentials of routing since the mobile ad-hoc networks are appreciably different from the wired networks. Furthermore, the conventional routing protocols of the Internet have been calculated for routing the transfer between wired hosts associated to a static backbone; in this manner, they can't be connected to impromptu

systems since the essential thought of such system is portability with dynamic topology [6]. Vehicular network challenges include technical problems like key distribution as well as more abstract difficulties, such as the need to appeal simultaneously to three very different markets.

a) Authentication versus Privacy: In a vehicular network, we would like to bind each driver to a single identity to prevent various other spoofing attacks. Strong authentication also provides valuable forensic evidence and allows us to use exterior mechanisms, for instance old-style law implementation, to identify or preclude attacks on some particular vehicular networks. Balancing privacy concerns with security needs will require practical considerations, codifying legal, as well as societal. Maximum countries have broadly divergent laws concerning their citizens' right to privacy [7].
b) Availability: For many applications, vehicular networks will require real-time, or near real-time, responses as well as hard real-time agreements. Even though some specific applications possibly will endure some margin in their response times, they will all characteristically necessitate faster retorts than those expected in traditional sensor systems, or even ad hoc networks.
c) Low Tolerance for Errors: Many applications use protocols that rely on probabilistic schemes to provide security. However, given the life-or-death nature of many proposed vehicular applications, even a quite small possibility of error will not be acceptable [8].
d) Mobility: For specifically vehicular types of networks, mobility is the standard, and hence it will usually be measured in miles, not meters, per hour. The mobility patterns of vehicles on the same road will exhibit strong correlations. Every particular vehicle will devour a persistently shifting set of neighbours, many of whom it has never interacted with before and is unlikely to interact with again [9].
e) Key Distribution: Key distribution is often a fundamental building block for security protocols. In vehicular networks, distribution poses several significant challenges. Vehicles are manufactured by many different companies, so installing keys at the factory would require coordination and interoperability between manufacturers. If manufacturers are unable or unwilling to agree on standards for key distribution, then we could turn to government-based distribution.
f) Incentives: Successful organisation of some vehicular networks will require incentives for vehicle manufacturers, consumers, and the government, and reconciling their often conflicting interests will prove challenging.

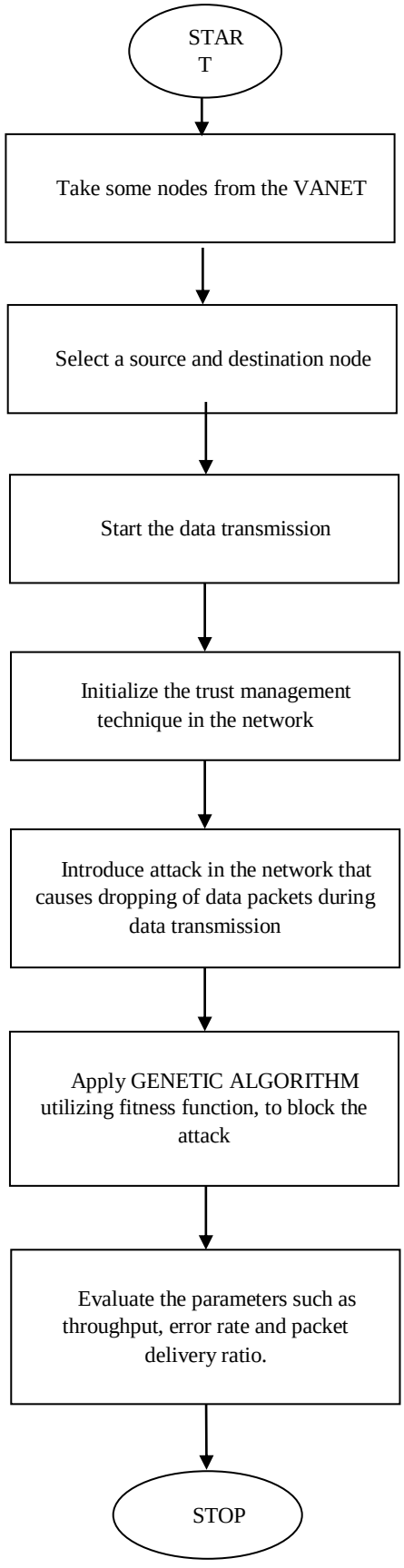
3. TRUST MANAGEMENT IN VANET

Modeling trustworthiness of peers in VANETs presents some unique challenges. Most importantly, the vehicles in a VANET are always roaming around as well as are highly dynamic. On a typical highway the average speed of a vehicle is about 100 kilometers an hour [10]. At high speeds the time to react to an imminent situation is very critical, thusly, it is critical for the peers to have the capacity to confirm/trust incoming data in real-time. Second, the quantity of peers in VANET can turn out to be huge. For example, in dense urban areas the average amount of vehicles that pass through go through the system may be on the request of millions and a few thousand vehicles will be expected to be present in the network at any given time. Additionally this circumstance is exacerbated amid the surge hours when, for instance, mainstream of the people commute to and back from work in a metropolitan area. This may introduce several issues some of which include network congestion - since vehicles are communicating on a shared channel, data overload - resulting from vehicles while getting a lot of data from the nearby vehicles in a congested area [11]. Hence there will be a need to have intelligent vehicle communication systems that are versatile and can identify and react to these possibly dangerous circumstances by adequately choosing with which peers to communicate. Another key challenge in modelling trust in a VANET environment is that a VANET is a decentralized, open system i.e. there is possibly no centralized infrastructure and also peers may join as well as leave the system at any time respectively. On the off chance that a peer is collaborating with a vehicle now, it is not ensured to interact with the same vehicle in the future [12]. Consequently, it is unrealistic to depend on systems that entail a centralized framework or social networks to construct long-term relationships. And in such an environment, there is much uncertainty in deciding whom to trust [13]. Also, information about road condition is rapidly changing in VANET environments, e.g. a road might be busy 5 minutes ago but now it is free, making it hard to detect if the peer spreading such information is malicious or not. This also brings out an important challenge that the information received from VANETs needs to be evaluated in a particular context. The two key context elements in VANETs are location and time. Information which is closer in time and location of an event is of more relevance [14].

4. *PROPOSED WORK MODEL*

The propose model work in following steps:

Step 1 : Take some nodes from the VANET.



Step 2 : Select a source and destination node from the given node.

Step 3 : Once, the nodes are selected start the data transmission.

Step 4 : Initialize the trust management in the network.

Step 5 : Introduce attack in the network, once attack on the network happens then it starts dropping data packets during data transmission.

Step 6 : Then apply Genetic algorithm to block the attack on the basis of using fitness function.

Step 7 : Evaluate the parameters such as throughput, error rate and packet delivery ratio.

Step 8 : Stop.

5. RESULTS AND IMPLEMENTATION

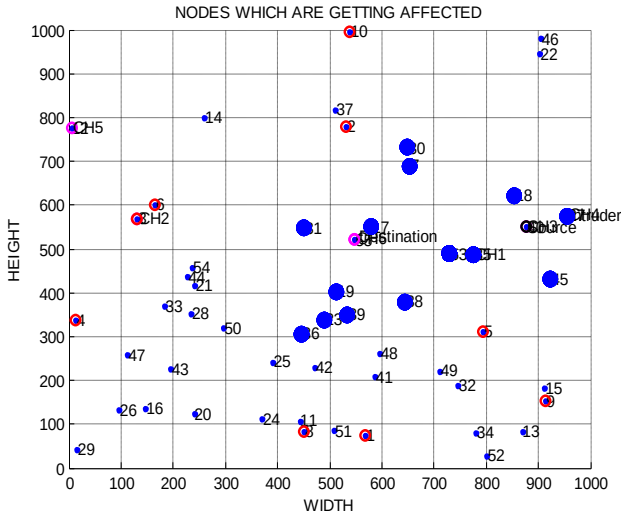


Fig. 2: *Network Deployment*

The above figure shows the simple VANET scenario that shows the node in blue color encircled with pink color representing cluster heads. Cluster heads are also abbreviated as CH. The red color nodes represents the affected nodes. The network is configured in 1000*1000 L* B area. It means height or width of network is 1000m. Cluster heads are chosen on basis of the residual energy every node in the network have equal probability of becoming cluster head. Every node in the network having some random energy nodes having maximum energy becomes cluster heads. From these cluster nodes we have consider one node as source node and destination node.

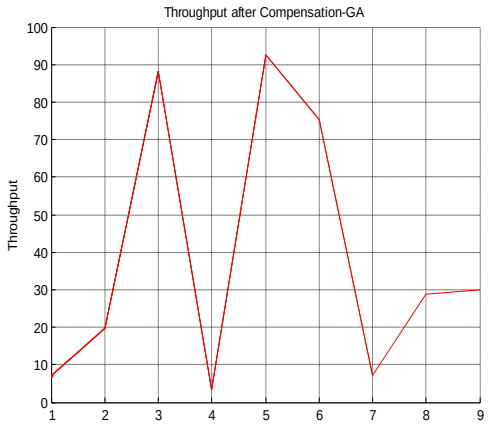


Fig. 3: *Throughput after Compensation using GA*

Now we have to analyze the throughput using genetic algorithm. In adhoc network throughput is measured as how many messages are sent over a channel out of them which are successfully reached at their destination. Or throughput is a measure of how many

units of information a system can Process in a given amount of time. The above figure shows the network throughput performance with compensation using Genetic algorithm with respect to the number of rounds and throughput is increased after applying GA which increases the network lifetime. In above given graph throughput versus no. of rounds is compared. Throughput gradually increases with no. of rounds.

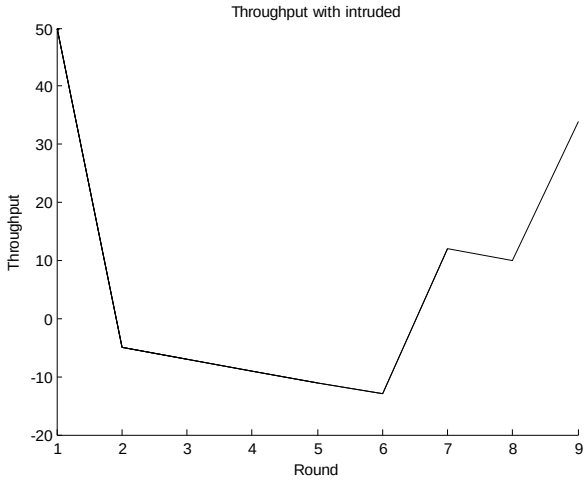


Fig. 4: *Throughput with Intruder*

An intruder is something that invades or system or networks without permission we don't even know that an interloper has arrived. Intruder in the VANET network violate the network properties below given figure shows the throughput with intrusion in the network. In this graph throughput and no. of rounds are evaluated. This shows when intruder invades in the network throughput starts decreasing with respect to no. of rounds.

The above figure shows the network throughput performance with attack compensation without Genetic algorithm with respect to the number of rounds. This shows the network performance violates when throughput get affected with the presence of the intruder in network. Intruder vanish the trustworthiness of the network.

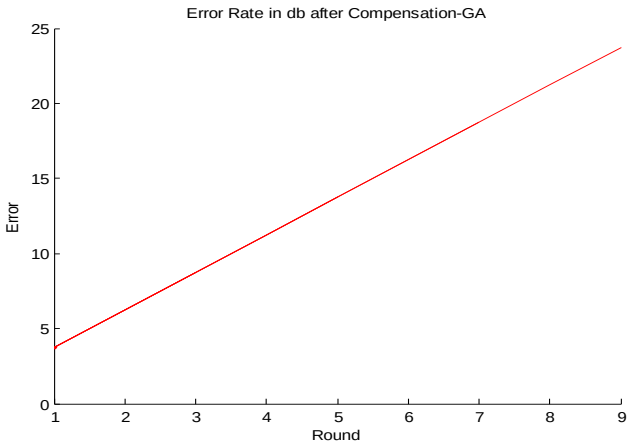


Fig. 5: Error rate after compensation using GA

Now we analyze the parameter error rate with intrusion or without intrusion in the network. Error rate is rate of error occurred in network when data is transmitting through a communication channel in the network if the error rate is high then network is less reliable. Mathematical formula of error rate is given below.

Error rate= total dropped packets/ packet count*100

Above given figure shows the compensation in error rate by using genetic algorithm. In the given figure error rate in db versus no. of rounds is compared. The above figure shows the error rate in the presence of attack and compensation using Genetic algorithm. The Error rate is more with attack which is compensated less after applying optimization algorithm.

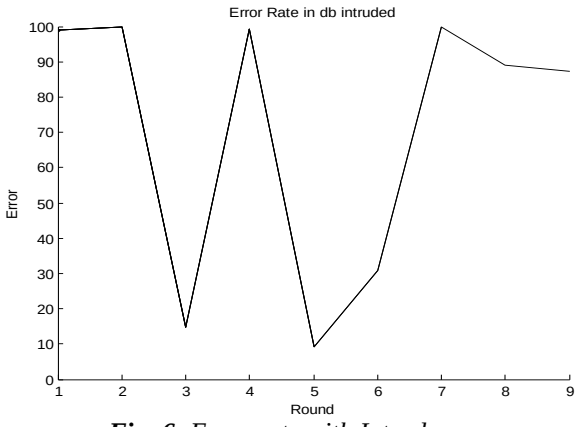


Fig. 6: *Error rate with Intruder*

Intruded error rate means how error rate of the network changes when intruder invades in the network. Error rates increases when intruder enters in the network and it violates the network properties and network life time. Trustworthiness of the network also gets affected. The above figure shows the error rate in the presence of intruder without GA.

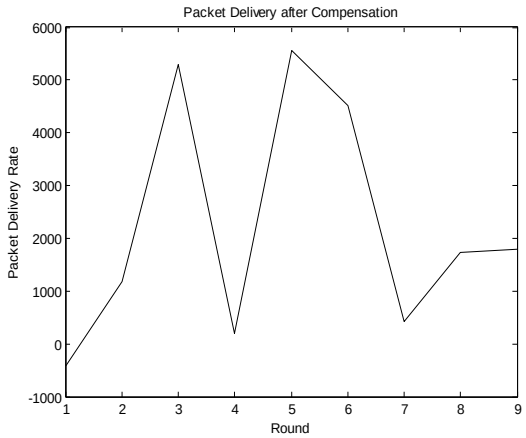


Fig. 7: *Packet Delivery after compensation*

Delivery rate or packet delivery rate is the rate of how many packets successfully received at their destination. Packet delivery rate mathematically illustrates as below. It is also abbreviated as PDR.

PDR=Number of packet receive/ Number of packets send

If packet delivery rate is higher it means network performance is higher.

The above figure shows the packet delivery rate with attack which is less i.e. the packet delivery to the destination is less due to attack and after applying GA the rate is increasing which should be high to increase the network lifetime. In figure no. of rounds versus delivery rate is given.

Fig. 8: *Intruder Packet delivery rate*

Above figure shows the delivery rate of messages with intrusion in the network. When intruder gets enter in the network packet delivery rate decreases and network life time also affected. The above figure shows the packet delivery rate with attack which is less i.e the packet delivery to the destination is less due to attack .

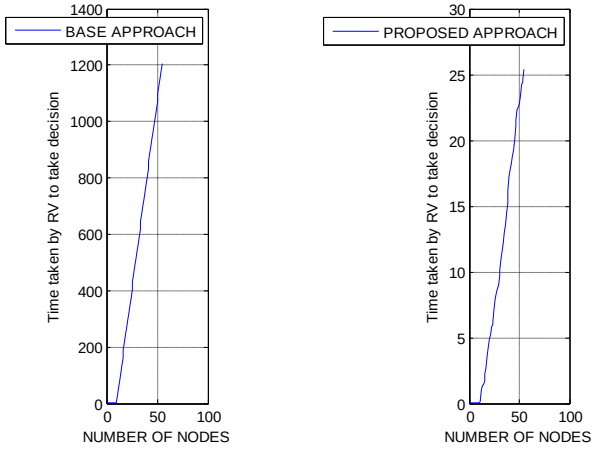


Fig. 9: *Time taken for decision making using proposed as well as base approach*

Above figure shows the time taken by required network for decision making in routing. From the graphs it has been concluded that proposed algorithm based on genetic optimization technique has less time consumption in terms of decision making in comparison without optimization.

6. CONCLUSION AND FUTURE SCOPE

In this work, we clearly identify the challenges in this environment, survey existing trust models proposed for different contexts, and point out their issues when being taken to the VANET domain. Then we propose a list of important properties that should be archived by trust management for VANET, setting a specific goal for researchers in this area. We also show the lack of effectiveness of the existing trust models for VANET, and draw particular attention to the robustness of trust models. Our research thus serves as one step closer towards the design and development of effective trust management for the deployment of safety, life-critical and road condition related systems by governments and business organizations to enhance road safety and reduce the number of car accidents and traffic congestion. The presented work is appreciable but it can be enhanced by removing the third party auditing from the network balance of which a lot of time is consumed and also the network does not remain as much as cost effective as it should be.

For future work, we will consider the presence of malicious leaders who intentionally drop messages. We will investigate a set of detection and revocation mechanisms to cope with this issue by dynamically selecting trustworthy leaders or introducing backup leaders.

REFERENCES

[1] M. Gerlach and F. Friederici. Implementing trusted vehicular communications. In Vehicular Technology Conference, 2009. VTC Spring 2009. IEEE 69th, pages 1 –2, april 2009.

[2] P. Papadimitratos, L. Buttyan, T. Holczer, E. Schoch, J. Freudiger, M. Raya, Zhendong Ma, F. Kargl, A. Kung, and J.-P. Hubaux. Secure vehicular communication systems: design and architecture. Communications Magazine, IEEE, 46(11):100 –109, november 2008.

[3] P. Ardelean and P. Papadimitratos. Secure and privacy-enhancing vehicular communication: Demonstration of implementation and operation. In Vehicular Technology Conference, 2008. VTC 2008-Fall. IEEE 68th, pages 1 –2, sept. 2008.

[4] J. P. Hubaux P. Papadimitratos, V. Gligor. Securing vehicular communications - assumptions, requirements, and principles. november 2006.

[5] F. Kargl, P. Papadimitratos, L. Buttyan, M. Muter, E. Schoch, B. Wiedersheim, Ta-Vinh Thong, G. Calandriello, A. Held, A. Kung, and J.-P. Hubaux. Secure vehicular communication systems: implementation, performance, and research challenges. Communications Magazine, IEEE, 46(11):110 –118, november 2008.

[6] M. Raya, P. Papadimitratos, and J.-P. Hubaux. Securing vehicular communications. Wireless Communications, IEEE, 13(5):8 –15, october 2006.

[7]

[8] P. Papadimitratos, L. Buttyan, J. P. Hubaux, F. Kargla, A. Kung, and M. Raya. Architecture for secure and private vehicular communications. 2007.

[9] T. Leinmüller, L. Buttyan, J. P. Hubaux, F. Kargl, R. Kroh, P. Papadimitratos, M. Raya, and E. Schoch. Sevecom - secure vehicle communication. june 2006.

[10] L. Buttyan and J. P. Hubaux. Security and Cooperation in Wireless Networks. http: //secowinet.epfl.ch, 2007. Cambridge University Press.

[11] C. Leckie and R. Kotagiri, "Policies for sharing distributed probabilistic beliefs," in Proceedings of ACSC, 2003, pp. 285–290.

[12] P. Papadimitratos and J. P. Hubaux. Report on the secure vehicular communications: Results and challenges ahead workshop. april 2008.

[13] D. Djenouri, W. Soualhi, and E. Nekka. Vanet's mobility models and overtaking: An overview. In Information and Communication Technologies: From Theory to Applications, 2008. ICTTA 2008. 3rd International Conference on, pages 1 –6, april 2008.

[14] S. D. Ramchurn, D. Huynh, and N. R. Jennings, "Trust in multi-agent systems," The Knowledge Engineering Review, vol. 19, no. 1, pp. 1–25, 2004.

[15] M. Gerlach, "Trust for vehicular applications," in Proceedings of the International Symposium on Autonomous Decentralized Systems, 2007