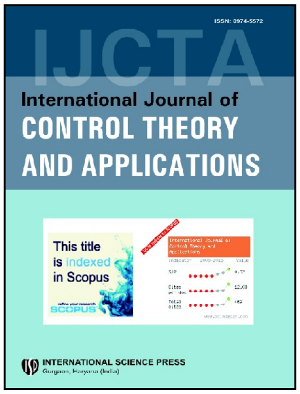


ISSN: 0974-5572

IJCTA

International Journal of CONTROL THEORY AND APPLICATIONS

This title is indexed in Scopus

INTERNATIONAL SCIENCE PRESS

International Journal of Control Theory and Applications

ISSN : 0974-5572

© International Science Press

Volume 10 • Number 11 • 2017

A Secure Cluster Based Framework for Preventing Attacks in Vehicular Cyber Physical System

Avani Mahajan[1] and Akwinder Kaur[2]

Department of Computer Science & Engineering, Chandigarh University, Mohali-140413, Punjab, India
E-mail: avanimahajan93@gmail.com
[2] Assistant Professor, Department of Computer Science & Engineering, Chandigarh University, Gharuan
E-mail: akwinderkaurkingra@gmail.com

Abstract: VANET(Vehicle Adhoc Network) is highly sensitive for attacks. Because these are DTN(Delay Torrent Network) which is highly frequency of Packet drops. So attack simulation in VANET is a very challenging process. We simulate five different attacks in VANET and detect these attacks by opportunistic network by throughput, delay and drop packet. Prevention of these attacksis done by Ant Colony optimization (ACO) with continue monitoring. The difference of parameters after detection and prevention shows in result part.

Keywords: VANET, attacks, detection, trust-centric parameters, prevention, ACO, one simulator.

INTRODUCTION

With the quick development of transportation, the number of road vehicles was improved beyond imagination; road traffic safety circumstances have become increasingly serious [1]. More than the past 10 years, a lot of research is dedicated to driving during the development of auxiliary systems to resolve the issues of traffic safety, this system can sense the vehicles, and exact repeat drivers when in danger [4].

Vehicular Ad hoc networks (VANETs) are a particular type of mobile ad hoc networks; where vehicles are simulated as mobile nodes. VANET restrains two entities: access points and vehicles, the access points are fixed and frequently connected to the internet, and they could contribute as a distribution point for vehicles [1]. VANET addresses the wireless communication among vehicles (V2V), and among vehicles and infrastructure access point (V2I). Vehicle to vehicle communication (V2V) has two types of communication: one hop communication (direct vehicle to vehicle communication), and multi hop communication (vehicle depend on other vehicles to retransmit). VANET also has particular characteristics that distinguish it from other mobile ad hoc networks; the most important features are: high mobility, self-organization, dispersed communication, road pattern limitations, and no restrictions of network size, all these features made VANETs environment a challenging for developing proficient routing protocols [1].

Indeed a rising number of vehicles are attached to Internet today; however they are largely joined via cellular networks only. The concept of connecting vehicles during Road-Side-Units (RSUs) has long existed, but only definite regions or countries deployed them. Standards have been enhanced for direct Vehicle-to-Vehicle (V2V) communication; however it is restricted to one-hop communication for collision prevention only. There have been various publications exploring the use of V2V to support a much broader range of applications; unfortunately those results are isolated point solutions using various patches to overcome the limitations of TCP/IP [3].

Vehicular networks can also be employed to present connectivity to remote rural communities and regions, enabling non-real time services, such as file-transfer, electronic mail, cached Web access, and telemedicine. Catastrophe hit areas lacking a conventional communication infrastructure can advantage from the deployment of a vehicular network to provide sustain for communication among rescue teams and assist communication between the rescue teams and other emergency services [9].

For the past few years, Delay and Disruption Tolerant Networking (DTN) has developed into a healthy topic in the field of networking technology. Numerous works have been done by the network designers and researches on DTN due to its intrinsic nature of the network. Even though researches on DTN started a decade ago, the principles, architecture and protocols have just been made concrete in recent times. Delay tolerant networks (DTNs), such as sensor networks with scheduled intermittent connectivity, vehicular DTNs that disseminate location-dependent information (e.g., local ads, traffic reports, parking information) [1], which makes routing quite distinctive from other wireless networks. Although various routing algorithms have been anticipated to increase data delivery reliability [9].

DELAY-TOLERANT networks (DTNs) have the capability to connect the nodes and have the aptitude to serve areas of the world that are being serviced by common networks. The prime difference among Internet and DTN communication is absent of end to end communication path which leads disconnection, variable delay, and high error rate in communication DTN uses store and forward concept to send message or packet from source to destination. DTN has numerous routing protocol based on information or replication strategy for successful delivery of packet from sender to beneficiary.Node store the message in its buffer memory until the next tenure-holder is found in the path towards to reach destination. Because of buffer size is limited node should follow some policy for choose which message is dropped in case of the buffer size is full [6].

VANETs are becoming the main appropriate wireless mobile technology. It is one of the promising approaches to implement Intelligent Transportation Systems (ITS). VANETs differ from MANETs in various ways: high node mobility, large scale of networks, a geographically constrained topology that is highly dynamic, strict real time deadline, unreliable channel conditions, unavoidably slow deployment, sporadic connectivity among nodes, driver behavior and numerous network fragmentations. A vehicular ad hoc network is a definite type of Mobile Ad hoc NETwork (MANET) that provides communication among nearby vehicles and roadside equipment In this type of network, vehicles are considered communication nodes that are able to belong to a self-organizing network without prior screening or knowledge of each other's existence There are two category of nodes: On-Board Units (OBUs) and Road Side Units (RSUs). OBUs are radio devices installed in vehicles that move, while RSUs are placed along the road and comprise the network infrastructure. RSUs work as a router among the vehicles. Using Dedicated Short Range Communication (DSRC) radios, OBUs can link the vehicle to RSUs[12].

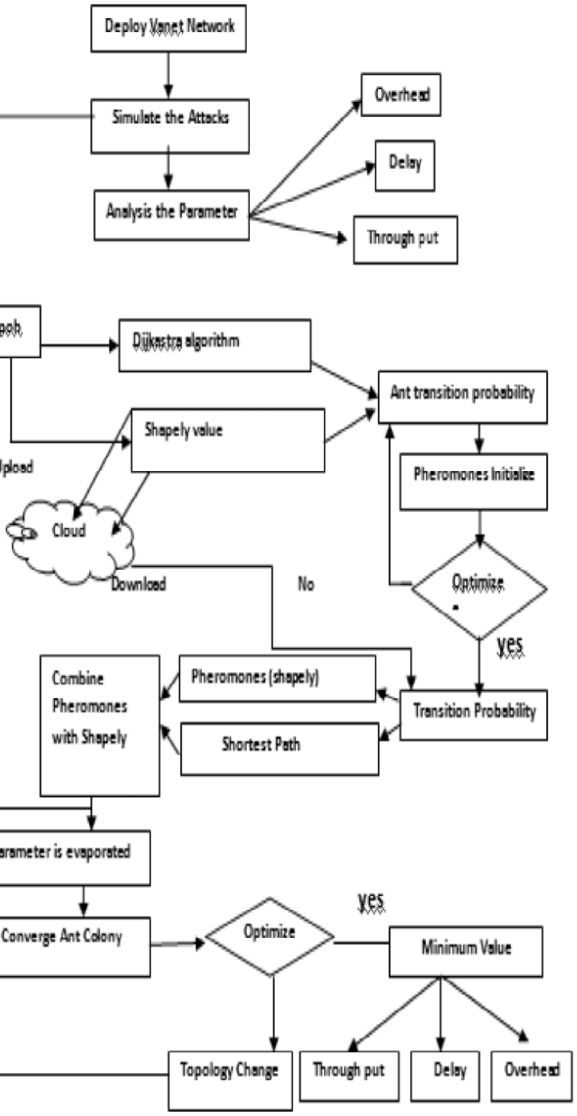
Therefore it is crucial that all the activities that are performed on VANET must be protected from malicious attacks. A number of novel problems are associated with a VANET is due to it's unique characteristics of the network. To begin, the main differences between a VANET and a MANET are a MANET typically has no infrastructure available. In the case of a VANET, it is achievable to tactically place access points along the side of the road, and consecutively consent to vehicles admittance to the services available from the infrastructure. Also, one of the greatest challenges is the vehicles in the network is mobility, speed of nodes is greater than the nodes in MANETs, leading to a network that can frequently become disjointed. Furthermore, security and privacy are essential apprehension for a VANET [3].

The introduction of new vehicular devices can really improve security in VANETs. Indeed, the provision of on-board Global Positioning System (GPS) devices has revolutionized driving. Correspondingly, the current introduction of short-range radar on some top-of-the-line models promises to decrease the number of fender–benders and other accidents. Interestingly, on-board radar is also used in superior cruise control systems [6]. It is natural, therefore, to enlist the help of these devices for the reason of enhancing the security of the information flow in VANETs. A classic example of ‘‘anti-social” behavior in VANETs is for spiteful cars to fake their true positions. Our prime contribution is to show that by using GPS and radar-provided information, one can make sure the validity of position information in a VANET and can detect and separate malicious cars [14].

[1] the traditional routing protocols in MANET is researched and the actual real movement of vehicles on the road is built for network simulation, all aspects of the performance of the AODV, DSDV and DSR routing protocols is analyzed in VANET environment, the result showed that the three classic routing protocols are not suitable for VANET with the haracteristic of low packet transmission rate, high normalized routing load and large delay in the average end to end. [2] presents a comprehensive survey of routing protocols proposed for routing in Vehicular Delay Tolerant Networks (VDTN) in vehicular environment and focused on a special type of VANET, where the vehicular traffic is sparse and direct end-to-end paths between communicating parties do not always exist. [3] provides an introductory overview of Vehicular Delay-Tolerant Networks. and an introductory description of applications and the most important projects is given. Finally, some research challenges are discussed and conclusions are detailed.[4] introduced position based protocols in VANET. The challenges and perspectives of routing protocols for VANET’S are finally discussed. Moreover, observed that carry-and-forward is the new and main consideration for designing all routing protocol n VANET’s. [5] represents the general outlines and goals of VANETs, investigates different routing schemes that have been developed for VANETs, as well as providing classifications of VANET routing protocols (focusing on two classification forms), and gives summarized comparisons between different classes in the context of their methodologies used, strengths, and limitations of each class scheme compared to other classes. [6] proposes a VDTN routing protocol, called GeoSpray, which takes routing decisions based on geographical location data, and combines a hybrid approach between multiple-copy and single copy schemes. [7] propose iTrust, a probabilistic misbehavior detection scheme, for secure DTN routing towards efficient trust establishment. The basic idea of iTrust is introducing a periodically available Trusted Authority (TA) to judge the node’s behavior based on the collected routing evidences and probabilistically checking. [8] proposes a clear and illustrative security architecture for DTN with secure key management framework to distribute the cryptographic keys to the constituted nodes in a secure way. [9] provides a summary on VANET and gives its routing protocols which focuses on vehicle to vehicle i.e. V2V communication and aims at classifying protocols on the basis of routing information and comparing them using following parameters namely methodology used, benefits/strengths and also compares reactive and proactive routing protocols based on their advantages and disadvantages, also discussing the challenges and research related issues for the routing mechanisms that exist in VANETs. [10] presents the pros and consof VANET routing protocols for inter vehicle communication. So, it is very necessary to identify the pros and cons of routing protocols which can be used for further improvement or development of any new routing protocol.[11] proposed system, enhancement is made with backward/forward secrecy technique, monotone access structure and escrows-free key protocol for security purpose and provides efficient management in confidential data.It describes these policies comprises of cipher- text policy attribute based encryption which permits to encrypt the confidential data using attributes or the public key. [12] addresses data delivery challenge in the possible intermittently connected vehicular sensor networks by combining position-based forwarding strategy with store-carry-forward routing scheme from delay tolerant networks. The proposed routing method makes use of vehicle driving direction to determine whether holding or forwarding the packet. Experimental results show that the proposed mechanism outperforms existing position-based solutions in terms of packet delivery ratio. [13] present some applications where VDTNs can be applicable and evaluate the suitability of the different proposals for each specific application. Moreover, identify a lack of realism in most of the simulation models used by the VDTN research community, providing certain guidelines to address this issue. [14] experimental performance evaluation of wireless communication, using IEEE 802.11 b/g, between boats in the Negro river. The main goal is to characterize the

transmission and the contacts of boats, aiming at evaluating the goodput of a delay tolerant network (DTN) formed by boats in the Amazon basin. [15] proposed a new Social-aware Vehicular DTN protocol (SocVe) respectively for a type of safety applications such as emergency support services. And conduct comparative performance evaluation of SocVe in multiple scenarios with different destination centralities against a geographical protocol. [16] aiming at tackling the critical issue of identity revocation, and introducing outsourcing computation into IBE for the first time and propose a revocable IBE scheme in the server-aided setting. And propose another construction which is provable secure under the recently formulized Refereed Delegation of Computation model. [17] exploration of the single-copy routing space in order to identify efficient single-copy solutions that (i) can be employed when low resource usage is critical, and (ii) can help improve the design of general routing schemes that use multiple copies. Also focused on some of the multi copy case techniques to decrease delivery ratio and delay. [18] presented a review of wireless access standards for VANETs, and describe some of the recent VANET trials and deployments in the US, Japan, and the European UnioN also briefly present some of the simulators currently available to VANET researchers for VANET simulations and we assess their benefits and limitations.

PROPOSED METHODOLOGY



Algorithm 1: Compute Shapley Value

```
Input: Opportunistic Network Topology
Output: Shapley value of all nodes in Network
Initialize the nodes by finding the Shapley value,
Begin
for each v ∈ V(G) do
        Distance Vector(D)=Dijkstra (v, G)
        ext.neighbour (v) = ø; extdegree (v) = 0;
        $d_{cut\_off}$ =0;
        for each u∈V(G) such that u ≠ v do;
              if D(u) ≤ $d_{cut\_off}$then;
                    extdegree (v)++;
              end for;
end for;
returnextdegree (v)++;
for each v ∈ V(G) do
        $sv(v) = \frac{1}{1+extdegree(v)}$;
        for each u∈ext.neighbour (v) do
              $sv(v) += \frac{1}{1+extdegree(v)}$;
        end for;
end for;
return(sv);
end;
```

Algorithm 2: Compute Minimum distance

```
Input: Opportunistic Network Topology
Output: Shortest distance ß$_d$
begin
        $D_s = 0$;
        $D_i = \infty$, for i ≠ s;
        ß$_d$= V;
        for i =0 to V=i
              findv$_m$∈ ß$_d$ with minimum d$_{m;}$
              for each edge (v$_{m ,}$ v$_t$) with v$_i$∈ ß$_d$
                    if((d$_i$ >d$_m$ )+ length (v$_{m ,}$ v$_t$)) then d$_i$ = d$_m$+ length (v$_{m ,}$ v$_t$);
              end for;
              ß$_d$=ß$_d$- v$_m$;
              end for;
        returnß$_d$;
end;
```

**Note:* Proposed algorithm take decision on the basis of shortest distance ß$_d$ andshapley value á$_s$, because *shapley value* represents the contribution of nodes in the network.

Algorithm 3 : Proposed Algorithm

Step 1. On the basis of algorithm 1ST and algorithm 2nd

Step 2. Take Random initialized path based on two parameters α_s and ß$_d$i. e. (D$_{1, d}$)

Step 3. Take the decision on the basis of α_s and ß$_d$

Step 4. Randomly send the data

$$P_{xy}^{k} = \frac{\left(T_{xy}^{\alpha_s}\right)\left(\eta_{xu}^{\beta d}\right)}{\Sigma_{Zallowed\ X}\left(T_{xz}^{\alpha_s}\right)\left(\eta_{xz}^{\beta d}\right)} \qquad \text{eq. 1}$$

where P_{xy}^{k} - moving from xto y on k probability

T_{xy}= pheromone deposited for transition from state x to y on α_s value.

η_{xy}= prior knowledge of shortest path depend on β_d value, assume $\beta_d \geq 1$

Step 5. Updation of T_{XY}

$$T_{XY} = (1-\rho)T_{XY} + \Sigma_k \Delta T_{xy}^{k} \qquad \text{eq.2}$$

ρ = negative prediction i.e. wrong path

k= kth time transmission of node

$$\Delta T_{xy}^{k} \qquad \text{eq.3}$$

$$\Delta T_{xy}^{k} = \begin{cases} \alpha / L_k \ ; \textit{if onetimeusesxypath} \\ 0; \textit{otherwise} \\ eq.3 \end{cases}$$

L_k = cost of shortest path (d) &shapley value (sv)

$$L_k = \alpha_s + ß_d \qquad \text{eq.4}$$

Step 6. Extract information of destination, find the path according to eq.1, eq.2, eq.3 and eq.4 & find the deviation in social information “T according to network domain

Step 7. Compute D$_{v, d}$ (new path) and D$_{1, d}$ (random path taken at starting)

If D$_{v, d}$< D$_{1, d}$

let v holds the message;

else L holds the message;

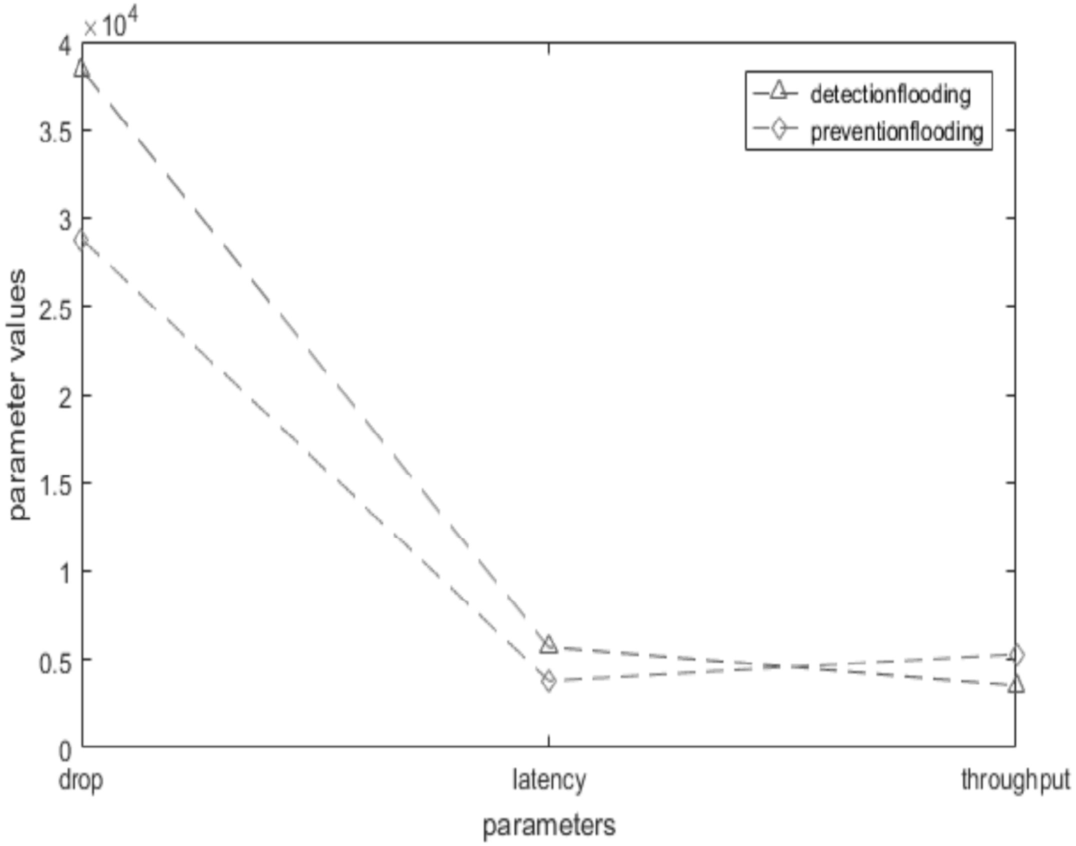
Step 8. End

RESULT ANALYSIS

Table 1
Flooding attack Preventation and Detectation

Parameters	*Prevention*	*Detection*
drop	28816.5	38422
latency	3808	5712
throughput	5308.11	3538.789

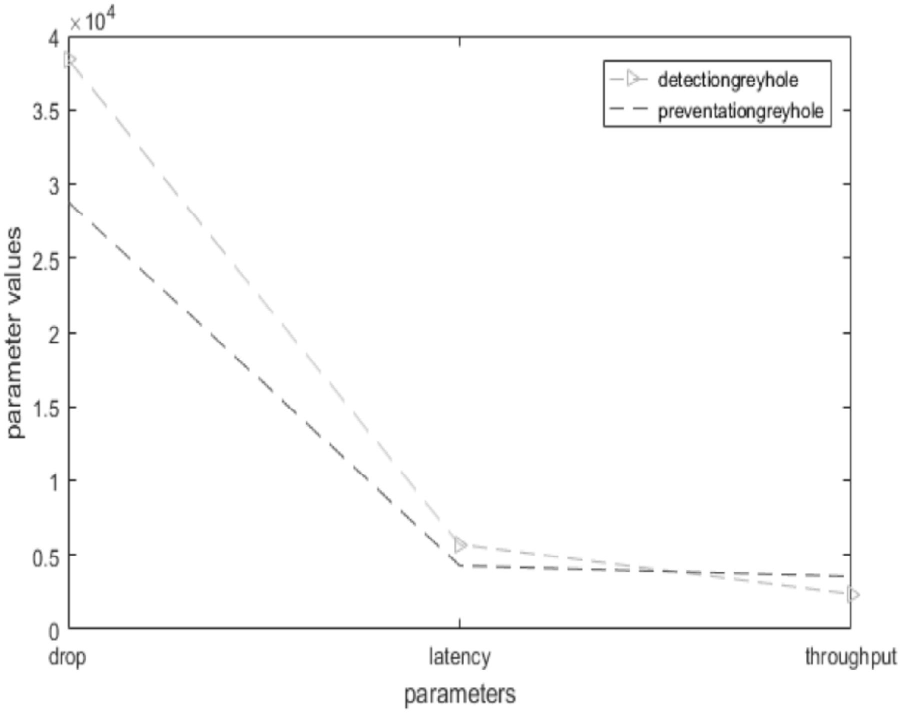
+



Graph 1: Comparison of preventation and detection in flooding attack

Table 2
Greyhole attack of preventation and detectation

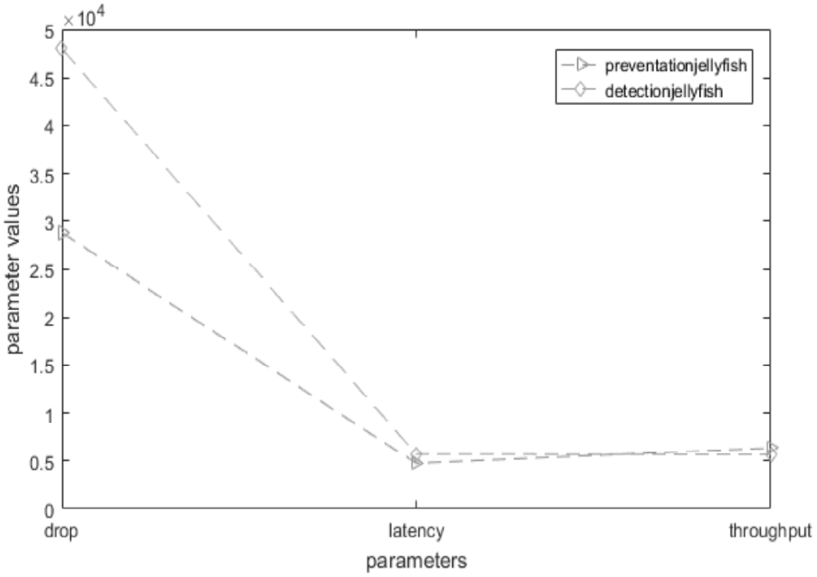
Parameters	*Prevention*	*Detection*
drop	28817.23	38422
latency	4284.2831	5713
throughput	3538	2359.16



Graph 2: Comparison of Greyhole attack of preventation and detectation

Table 3
Jellyfish attack of Preventation and Detectation

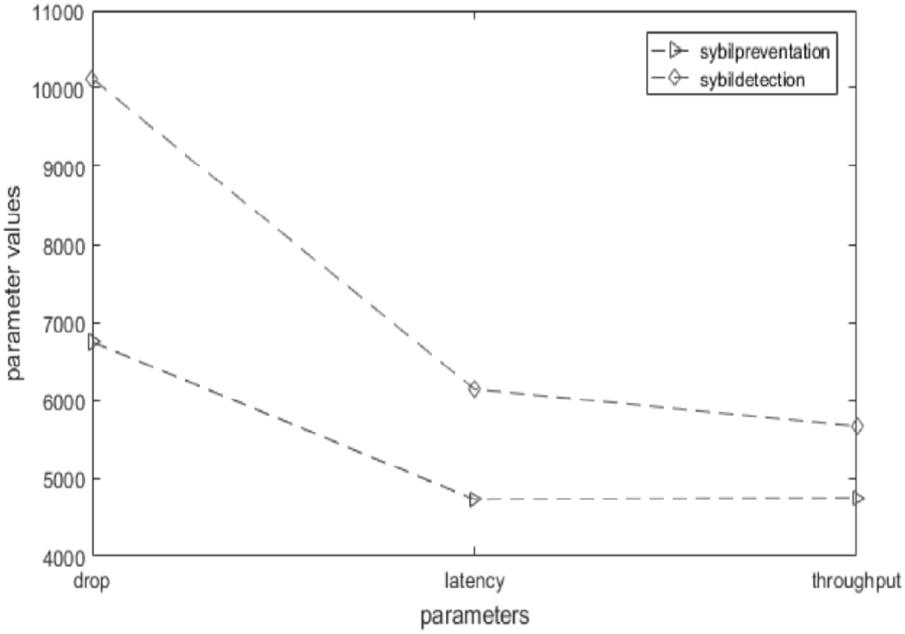
Parameters	*Prevention*	*Detection*
drop	28818	48027
latency	4760.3145	5714
throughput	6369.733	5661.98



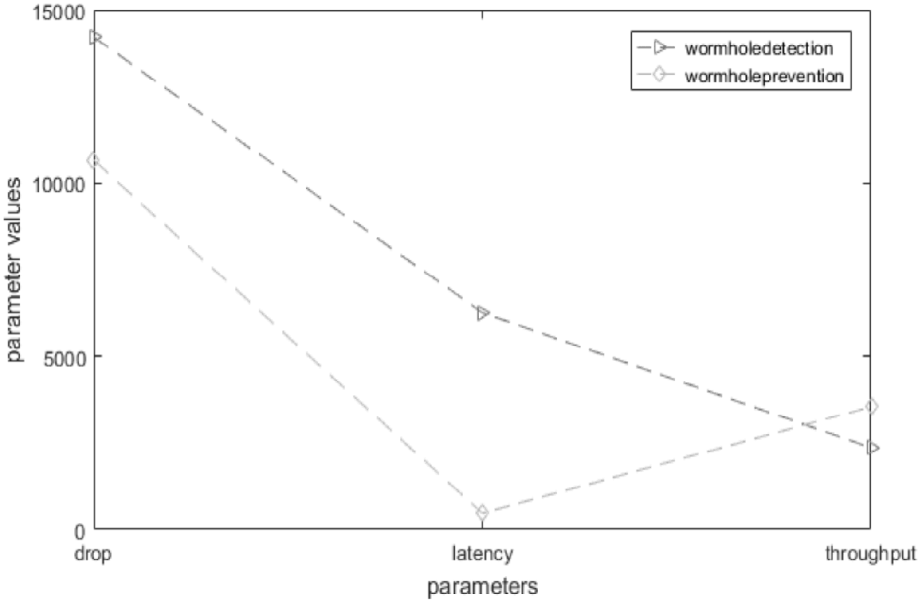
Graph 3: Comparison of Jellyfish attack of Preventation and Detectation

Table 4
Sybil attack of Preventation and detectation

Parameters	*Prevention*	*Detection*
drop	6748	10122
latency	4723.58	6140
throughput	4738.722	5661.98



Graph 4: Comparison of Sybil attack of Preventation and detectation



Graph 5: Comparison of Wormhole attack of Preventation and detectation

Table 5
Wormhole attack of Preventation and detectation

Parameters	*Prevention*	*Detection*
drop	10660.5	14214
latency	469.9635	6259
throughput	3541.78	2361

CONCLUSION

In this paper we have simulated five different attacks Flooding, Jellyfish, Greyhole, Sybil and wormhole attacks. We have shown the parameter analysis in detection and prevention. Prevention use Ant Colony optimization and optimize the parameters like drop, latency and throughput. Conclusion of this paper is that Ant Colony method shows significant optimization of the parameters and approximate real time monitoring.

REFERENCES

[1] Zhu, D., Cui, G., & Fu, Z. (2014). DT-AODV: An On-Demand Routing Protocol based DTN in VANET. *Applied Mathematics & Information Sciences*, *8*(6), 2955.

[2] Benamar, N., Singh, K. D., Benamar, M., El Ouadghiri, D., & Bonnin, J. M. (2014). Routing protocols in vehicular delay tolerant networks: A comprehensive survey. *Computer Communications*, *48*, 141-158.

[3] Pereira, P. R., Casaca, A., Rodrigues, J. J., Soares, V. N., Triay, J., & Cervelló-Pastor, C. (2012). From delay-tolerant networks to vehicular delay-tolerant networks. *IEEE Communications Surveys & Tutorials*, *14*(4), 1166-1182.

[4] Altayeb, M., & Mahgoub, I. (2013). A survey of vehicular ad hoc networks routing protocols. *International Journal of Innovation and Applied Studies*, *3*(3), 829-846.

[5] Soares, V. N., Rodrigues, J. J., & Farahmand, F. (2014). GeoSpray: A geographic routing protocol for vehicular delay-tolerant networks. *Information Fusion*, *15*, 102-113.

[6] Swetha, B., Rao, D. B., & Rao, P. N. (2014). Intelligent Anti-Theft Finding Scheme Towards Itrust Establishment in Delay Tolerant Networks Using VANET.

[7] Rajan, G., & Cho, G. (2015). Applying a Security Architecture with Key Management Framework to the Delay/Disruption Tolerant Networks. *architecture*, *9*(4).

[8] Dhankhar, S., & Agrawal, S. (2014). VANETs: A Survey on Routing Protocols and Issues. *International Journal of Innovative Research in Science, Engineering and Technology*, *3*(6), 444-463.

[9] Paul, B., Ibrahim, M., Bikas, M., & Naser, A. (2012). VANET routing protocols: Pros and cons. *arXiv preprint arXiv:1204.1201*.

[10] Veena, S., & Manjula, V. (2016). Effective Data Retrieval in Disruption Tolerant Networks Using Cipher Text Policy-Attribute Based Encryption. *Indian Journal of Applied Research*, *5*(6).

[11] Li, F., Zhao, L., Fan, X., & Wang, Y. (2012). Hybrid position-based and DTN forwarding for vehicular sensor networks. *International Journal of Distributed Sensor Networks*, *2012*.

[12] dos Santos, A. D. J., Braga, M. D. L., Velloso, P. B., Jose, G. R., & Costa, L. H. (2014, September). Capacity analysis of a delay and disruption tolerant network in the Amazon basin. In *2014 Global Information Infrastructure and Networking Symposium (GIIS)* (pp. 1-6). IEEE.

[13] Li, J., Li, J., Chen, X., Jia, C., & Lou, W. (2015). Identity-based encryption with outsourced revocation in cloud computing. *Ieee Transactions on computers*, *64*(2), 425-437.

[14] Patel, D., & Shah, R. (2016). Improved PROPHET Routing Protocol in DTN.

[15] Zeadally, S., Hunt, R., Chen, Y. S., Irwin, A., & Hassan, A. (2012). Vehicular ad hoc.

[16] Rasheed Hussain, Heekuck Oh. (2014). On Secure and Privacy-Aware Sybil Attack Detection in Vehicular Communications.

[17] Anees Ara, Mznah Al-Rodhaan,Yuan Tian, Abdullah Al-Dhelaan (2015). A Secure Service Provisioning Framework For Cyber Physical Cloud Computing Systems.

[18] Rasheed Hussain, Sangjin Kim, and Heekuck Oh (2012). Privacy-Aware VANET Security: Putting Data-Centric Misbehavior and Sybil Attack Detection Schemes into Practice.