Volume 6, Issue 9, September 2016 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

An Effective and Secure Routing Technique for VANETs

Richa Rani[1], Kamaljeet Kaur Mangat[2]
[1] M.Tech Student, [2] Assistant Professor
[1, 2] Department of CSE, Punjabi University Regional Centre for Information Technology and Management, Mohali, Punjab, India

Abstract*: Wireless network have seen a wirespread adoption in the standard systems. Vehicular ad-hoc network is a self configuring infrastructure less network of mobile devices connected wirelessly for communication. These networks are vulnerable to various attacks such as sleep deprivation attack. These attacks affect the communication between the number of the vehicles or nodes. There is a need of a technique that can prevent the network from these security attacks. The proposed work implements CBDS with the help of PSO algorithm to palliate sleep deprivation attack. The network parameters used are throughput, delay and jitter to evaluate the performance of the algorithm under different scenarios.

***Keywords*— Sleep deprivation, reverse tracing, CBDS, Security, PSO Algorithm**

I. INTRODUCTION

Wireless networks play a very eminent role in day to day communications. It have seen widespread adoption in the standard security system. Vehicular ad-hoc Network is special kind of wireless mobile ad hoc network that has the characteristics of mobility of high nodes and rapid changing topology[1]. VANET is a self-configuring, infrastructure-less network of mobile devices connected wirelessly for communication. VANET provides a wireless communication among nearby vehicles and roadside units. In VANET, vehicles use vehicle to vehicle (V2V) and vehicle to roadside (VRC) communication to interact with each other and with the existing roadside units. The performance of VANET routing protocls depend on various parameters like system throughput, end to end delay, routing overheads[2]. Security is one of the major concern in VANET as these networks are vulnerable to various attacks such as Sleep Deprivation, black hole attacks. There exist high need to secure the network from various attacks for deployment and its use in real life scenarios.

Sleep Deprivation attack has now become a major threat to current networks. It has become a dangerous attack[4]. Various mitigation techniques and defense mechanisms are proposed for Sleep Deprivation attack. Some of these techniques degrade the network performance by consuming the available resources. There is a need to secure the networks from these type of attacks.

In this paper, an efficient and secure routing technique is developed, which protects the network. The proposed technique simulates the CBDS scheme to protect the network from Sleep Deprivation Furthermore it improves the security of the CBDS scheme with the help of Particle Swarm optimization. The simulation of the network has been done using MATLAB simulator. The evaluation is done on the basis of performance parameters such as throughput, end to end delay and jitter.

II. LITERATURE REVIEWS

The open research areas have been discussed in which VANET introduce a new challenging environment for the communication engineers and developer. The author provides an overview of the issues in the VANET. It describes the VANET applications for safety and entertainment purpose and some research areas are discussed that need to be addressed still to enable the deployment of the technologies in the VANET[9].

The research challenge that need to be addressed for the quick deployment and adoption of the reliable, scalable, secure, robust VANET protocols, architecture, technologies and services. There are various threats to the availability, confidentiality, authenticity in the VANET where the no. of the attacks are identified such as black hole attack, DOS aatack etc. An offender can target the network layer of VANETs. Attacks on routing plane target the routing process of the network, while data plane attacks target the path forwarding practicality of the network The several VANET simulation models and tools are also defined[3].

ART (An attack resistant trust management scheme) is proposed, for VANET that is able to detect and cope with the malicious nodes and the attacks for securing the routing process. The author also evaluate the trustworthiness of the data and node in vehicular ad-hoc network. The ART scheme is applicable to the wide range of VANET that improves the traffic safety, effectiveness and trustworthiness of the nodes in VANET and it can also cope with the mallicious attacks[12].

A hash based scheme is presented to mitigate the sleep deprivation attack in the network. The two more schemes are also described that are round robin scheme and random vote scheme. These schemes are able to reduce the adversary attack but in these schemes, the amount of time is required to select a cluster of nodes and the huge amount of energy is required to perform these schemes. Out of these schemes, hash based scheme is superior in terms of the recovery from the attacks in the network[6].

Distributive collaborative mechanism, a hierarichal framework, proposed to detect the sleep deprivation attack in the wireless sensor network. To attain this, they uses a anomaly detection technique to reduce the intrusion of the false nodes. To mitigate the attack, the distributive collaborative mechanism physically excludes the malicious nodes from the network and rejects the fake data and packets. From this, the lifetime of the network is extended as the power consumption by the sensor nodes is reduced[4].

The collaborative/grayhole attacks in the mobile ad-hoc network by implementing CBDS (cooperative biat detection scheme) and analysis of these attacks are conducted. In the network, identifying the malicious node is a challenge from where security of network become a major concern. As a result, CBDS scheme is used to detect the malicious node in MANET. So, it is found that the proactive and reactive defense architecture includes in CBDS detects and prevents the malicious nodes in the mobile ad-hoc network[5]

III. PROPOSED WORK

A high need of security in routing protocols for the well organized routing due to which there will be less unplanned of packet drops and high delivery of packets with less delay from source to destination . Routing protocols need to be secured for the effective routing to overcome the issue of the delay of packets[6]. The Sleep deprivation attack and their protection is one of the major concerns which needs to be solved.A need of algorithm that is effective and quick to prevent from these attacks [5].

IV. PROPOSED SOLUTION

In the proposed work the Sleep deprivation attack is eliminated by black listing of malicious node after detection of node as malicious and non malicious. The figure below gives an idea of the elimination of malicious nodes after the identification of malicious nodes by using the CBDS technique and improving and optimizing the reverse tracing process of CBDS with the help of PSO Algorithm. Reverse tracing technique,the detection message will be send to the nodes which is a secret message that will help to detect the malicious nodes. Now the nodes other than malicious nodes will not reply to the source node as the favour message is a secrect message for the detection of the malicious node which defines to not send the reply back to the source node in the next request.

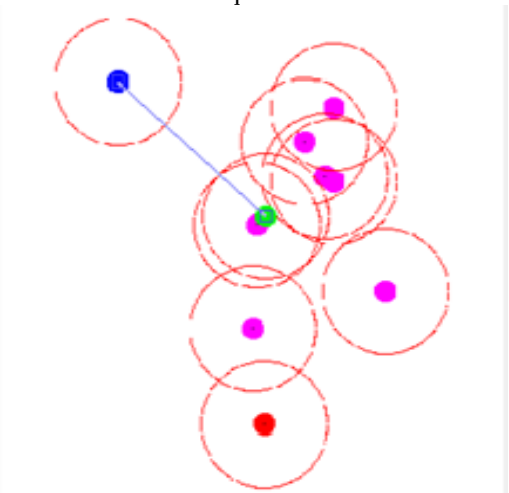

Fig 4.1 Simulation of the system

The discussion of the simulation starts form the initial steps of network setup involving the node deployment with number of nodes and the network basic setup for routing. After the initial setup the nodes are used to simulate the time based sleep scheduling in the first place for the normal scenario. The network is given a source and a destination as input and the routing of the packets start from the source to the sink. Then the network simulation of the Sleep deprivation attack is done in which the some nodes are given the properties of the attacker. With the use of CBDS ,the identification of the attacker is done. In reverse tracing technique, the detection message will be send to the nodes which is a secret message that will help to detect the malicious nodes. Now the nodes other than malicious nodes will not reply to the source node as the favour message is a secrect message for the detection of the malicious node which defines to not send the reply back to the source node in the next request. As nodes donot send the reply to the source node, only malicious nodes send the detection message reply to the source node, which help the source node to identify fake nodes.The failure of the nodes in authentication process make them invalid and black listed in the future premises, Some brute force attack are also assumed in the network by which the malicious node can break the CBDS reverse tracing technique. So it requires the use of PSO algorithm for optimization in order to improve the results. The below fig 4.2 denotes the steps involved in implementation of algorithm

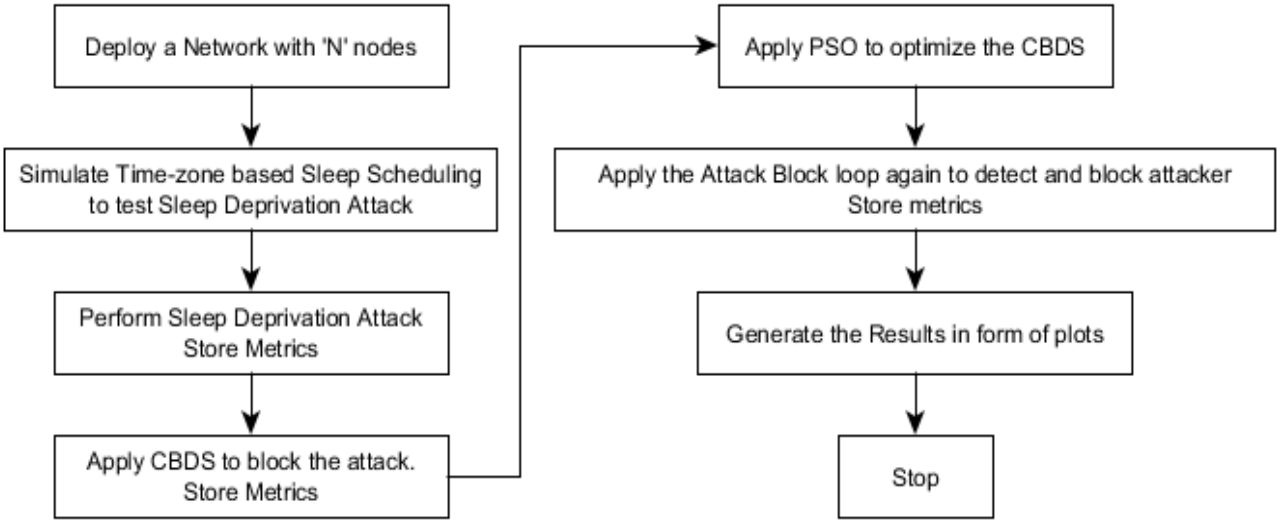

Fig 4.2 . Block diagram of Methodology

V. SIMULATION RESULTS

The CBDS is optimized with the help of PSO algorithm has been simulated using MATLAB simulator. The performance metrics required to evaluate the results of the implemented algorithm are discussed in this chapter. Further, results of the proposed method as obtained are evaluated on the basis of selected parameters and the validation of the proposed system is discussed. The performance is analyzed on the basis of parameters such as throughput, end to end delay and jitter. The performance of algorithm has been analyzed under different scenarios with variable number of nodes.

Figure 5.1 shows the graph between the Throughput and the number of rounds. This is a cumulative graph in which the rounds are simulated and the result are added.

Throughput=Number of packet/Time taken

Throughput is decreased to low level during the attack. It can be depicted from graph indicated by blue line that improvement in throughout occurs due to the use of CBDS technique. Throughput is further improved as CBDS is optimized with the help of PSO.

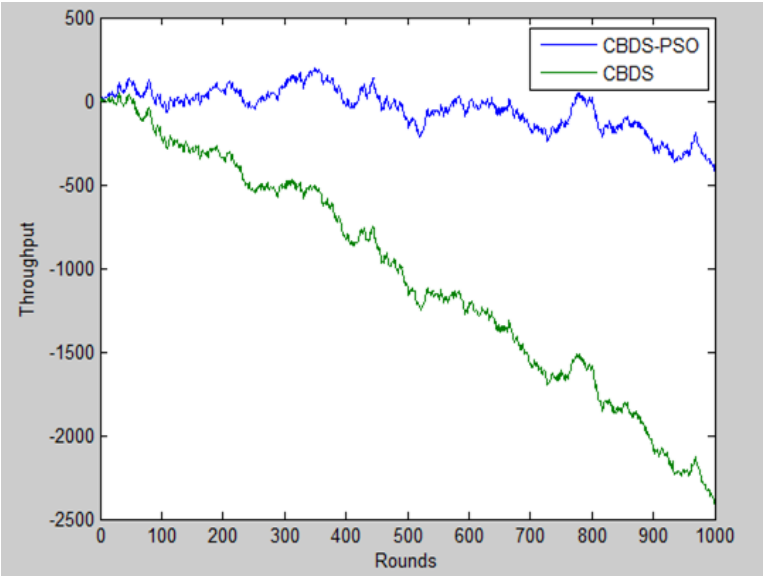

Figure 5.1: Throughput comparison

End to end delay is time taken by the packet to be transferred from source to destination. Figure 5.2 represents the results of End to End Delay of the system. The end to end delay significantly losses it value during the attack because the packet transfer is stopped. With the use of CBDS, the packets start to route again and the malicious nodes are black listed. Due to the avoidance of malicious nodes, the delay of packet also decreases with the use of CBDS and PSO Algorithm. As with the only CBDS technique, the end to end delay increases because the optimization algorithm was not involved to increase the performance of the vehicular nodes but the performance of vehicular nodes improved only when the CBDS technique is optimized the PSO algorithm which black lists the malicious nodes and ignore it. So, the performance of the end to end delay is improved and the end to end delay of the delievery of packets decreases with the use of CBDS technique which is optimized with the help of PSO algorithm. The blue line shows the improved result with the use of the CBDS technique optimized with the PSO algorithm.

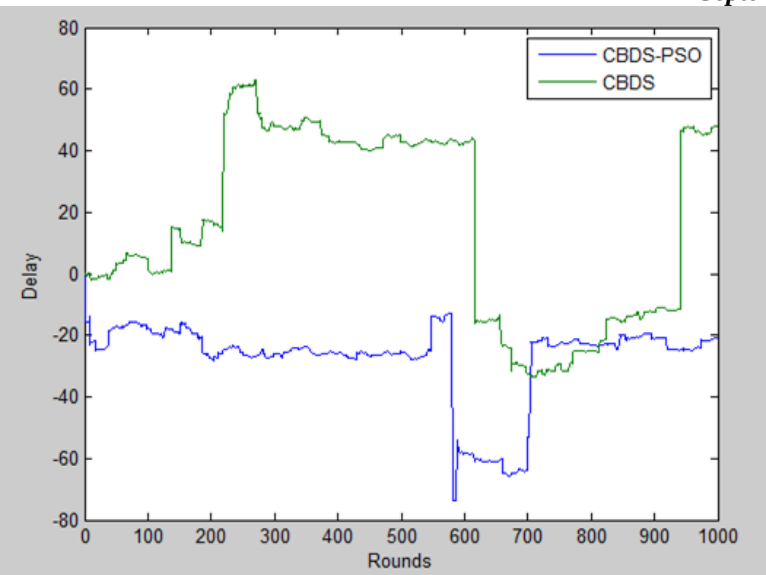

Figure 5.2: End to end Delay comparison

Jitter is outlined as a variation within the delay of received packets. Figure 5.3 represent the jitter in the network. The jitter like end to end delay losses its value during the attack due to the unavailability of the packets. The blue lines shows that delay is recovered by sending the another packet at the same time. So, Jitter also improves with help of CBDS and further by the use PSO Algorithm.

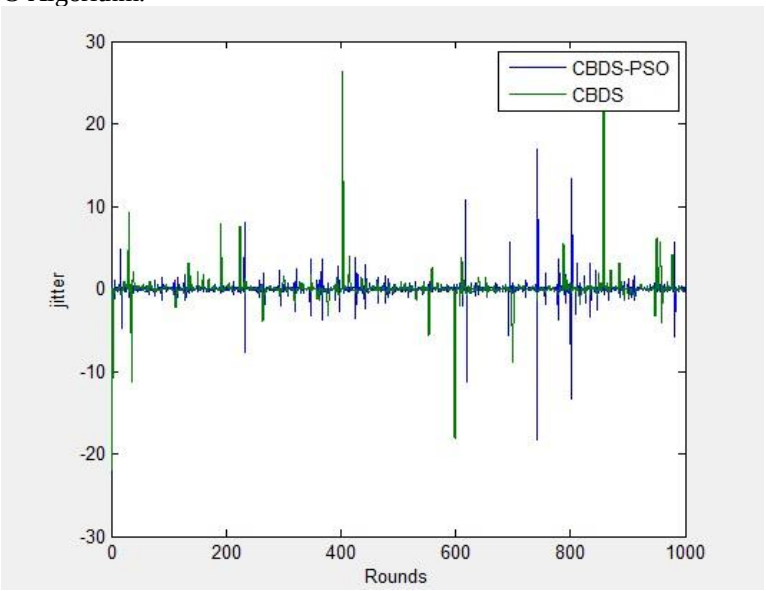

Figure 5.3: jitter comparison

Figure 5.3 shows the comparison of Jitter of the CBDS-PSO scheme and CBDS only scheme. The jitter in CBDS-PSO scheme has a spike in 700th round. This point shows the delay in the packet sending dur to the detection of malicious node with the use of CBDS when spike goes upward but at the same time, delay recovers by sending the another packet when spike goes downward. This shows that CBDS-PSO scheme has optimized search time for the malicious node and thus can detect the malicious node very fast and thus protect the network from sleep deprivation attack in a more optimized manner.

The algorithm has been implemented and validated under different network scenarios.Three simulation scenarios have been designed containing the varying number of nodes . The description of these scenarios is given as

Scenario-1: 200
Scenario-2: 400
Scenario-3: 600

Table 5.1: Performance of CBDS optimized with PSO algorithm in networks of variable size

Scenarios	Scenario 1	Scenario 2	Scenario 3
Throughput	**8.764**	**8.483**	**8.217**
End to End Delay	**1.12**	**1.17**	**1.21**
Jitter	**-4.6**	**-3.8**	**-3.5**

The three scenarios where scenario 1 contains 200 nodes, scenario 2 contain 400 nodes and scenario 3 contain 600 nodes. Table 5.1 shows the quantative values of the performance of CBDS optimized with PSO algorithm having different no. of nodes. The value of the parameter of end to end delay increases as the no. of the nodes increases in network. Throughput decreases as the traffic increases in the network.

VI. CONCLUSION AND FUTURE SCOPE

The work done in this thesis shows elimination of malicious nodes with the help of CBDS scheme and PSO algorithm. The simulation of the network was done in MATLAB with the effect during the Sleep deprivation attack. We identified the malicious nodes and then black listed them at the time of the routing process. PSO algorithm was applied to improve the reverse tracing technique of the CBDS scheme. The results show significant improvement with the use of CBDS optimized with use of PSO Algorithm. The MATLAB simulation showed the use of CBDS can be valid option in blacklisting of nodes. The misconception of the extra time taken by CBDS is removed as the extra bit of time taken by the algorithm is very beneficial for the overall performance of the network. The performance was analyzed and checked on various parameters like throughput, end to end delay and jitter. The performance of CBDS optimized with PSO algorithm is validated under different scenarios in terms of variable number of nodes. The algorithm performs better in terms of all parameters. It provides much greater performance and handles the security of network.

An effective and secure routing technique is realized in this work. Though this technique helps in making the network more reliable however this approach can further be extended.

Security feature has attracted many researchers. In this study the CBDS scheme combined with PSO algorithm is applied to protect against Sleep deprivation attack. The implementation of algorithm can be tested against certain other network attacks such as black hole attacks. Study can be extended to be applied in various application scenarios such as for secure deployment of UAV (unmanned aerial vehicle), deployment of IP services .The algorithm can be tested and validated for a variety of networks such as wireless mesh network.

REFERENCES

[1] Maxim Raya, and Jean Pierre Hubaux. "The security of Vehicular ad-hoc network" *IEEE Transaction*,vol 15,no. 3, pp 212-64,2016

[2] Ghassan Samara "Security analysis of vehicular ad-hoc network" *International conference on communication*,vol 13,no. 4,pp 1765-1780, 2015

[3] Sherali Zeadally "Architecture and algorithm based VANET", *IEEE transaction*,vol 10,no. 3,pp 171-84,2014

[4] Tapalina bhattasali "*Sleep* deprivation attack detection in wireless sensor network" *International journal of computer communication*,vol 40,no 15,pp 789-812,2012

[5] Akinlemi Olushola "Detection of attacks using CBDS" *IEEE Transaction*,vol 20,no.4,pp 141-156,2012

[6] Mathew Pirreti and Sencun Zhu "The sleep deprivation attack in sensor network", *IEEE transaction*,vol 40,no. 7,pp 10-15,2014

[7] Vinh Hoa LA, Ana Cavalli "*Security Attacks and Solutions in Vehicular Ad hoc Nwtworks*" Vol. 4, No. 2,pp.356-368, April 2014

[8] RG. Engoulou, M. Bellache, S. Pierre, and A. Quintero, "VANET security surveys," *Comput. Commun.*, vol. 44, no. 0, pp. 1–13, May 2014.

[9] Md. Humayun Kabir, "Research issues on vehicular Ad Hoc Network" IEEE Transaction,vol. 4,no. 4, pp. 231-381,dec 2013.

[10] Chethan kumar KM "CBDS for detection, prevention launching in the network" *International journal of engineering research*,vol 5,no. 4,pp 790-991,2016

[11] S.Al-Sultan, M. M. Al-Doori, A.H.Al-Bayatti, and H. Zedan, "A comprehensive survey on vehicular ad hoc network," *J. Netw. Comput. Appl.*,vol. 37, no. 1, pp. 380–392, Jan. 2014.

[12] Li Wenjia, and Houbing Song "ART: An Attack-Resistant Trust Management Scheme for Securing Vehicular Ad Hoc Networks", *IEEE Transaction*,vol.17, no. 4, pp. 1950-64,2015

[13] B.T.Sharef, R.A.Alsaqour, and M.Ismail, "Vehicular communication ad hoc routing protocols*: A survey*," *J. Netw. Comput. Appl.*, vol. 40,pp. 363–396, Apr. 2014.

[14] Zhu, Hongzi "Impact of traffic influxes: Revealing exponential intercontact time in urban vanets." Parallel and Distributed Systems, IEEE Transactions, vol 22, pp.1258-1266,2011

[15] Alpcan,Tansu and Sonja Buchegger. "Security games for vehicular network." *Mobile Computing, IEEE Transactions*, vol 10, pp.280-290, 2011

[16] Lin, X. Sun, P.-H. Ho, and X. Shen, "*GSIS: A secure and privacy preserving protocol for vehicular communications*," *IEEE Trans. Veh. Technol*, vol 56, pp. 3442–3456, 2007

[17] Dotzer F, Fischer L, Magiera P, "Vars: a vehicle ad-hoc network reputation system," *IEEE international symposium on a world of wireless mobile and multimedia networks*, vol 34, pp.454–456,2005

[18] Jalil, K.A., Ahmad, Z. and AbManan, J.L, "Securing Routing Table update in AODV routing protocol" *International journal of computer communication Transaction*,vol 12,no. 4,pp 178-191,2011.

[19] Khelifa, S.Maaza, Z.M, "An energy multi-path AODV routing protocol in ad hoc mobile networks" *International Symposium on* IEEE,pp 1-4,2010.

[20] Manish Poonia, "Danger Theory Based Model to Prevent Sleep Deprivation Attacks in MANETs" *IEEE Transaction,* vol 13,no.5,pp 12-17,2014.

[21] Vinothini, A.T. and Madhurikkha, "A Secure Scheme Using Priority Based Scheduling and Congestion Control (PBSCC) Protocol to Avoid Sleep Deprivation Attack in MANET" *International jouranal of research*,vol 20,no. 5,pp 771-782,2010

[22] J. Lemon. "Resisting SYN Sleep attacks with a SYN cache", in *Proceedings of USENIX BSDC*,pp. 89-98,Feb. 11-14, 2002.

