INTERNATIONAL JOURNAL
FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Secure Data Transmission in Mobile ADHOC Network with Verification of Neighbor Positions

Priyadarshini. P[1], Mr. Prabhu. S[2], Ramadevi. S[3]

[1, 3]Student, [2]Professor, Department of Computer Science and Engineering, S. A Engineering College

Abstract: Mobile adhoc network is a wireless, infrastructure less and dynamic wireless network in which node contain the resource. In MANET, all mobile work agreeably to find route and transfer the information to the destination. When all nodes transmit the data at the same time traffic occur in the network and this is the tedious process in the MANET.IDS instruction detection system is used to monitor the process taking place in the network between the nodes. The IDS should be always active in all nodes in all time. It monitors the events taking place in the network system. In our proposed system, we ensure data transmission in efficient ways and reduce the effectiveness of the IDS.
Keywords: MANET, Security, IDS, Network, packet delivery.

I. INTRODUCTION

Mobile adhoc network is infrastructure less and security is the main draw back in this MANET network and to secure the data transmission in network and using intrusion deduction system to detect and eliminate the attackers from that specific route. Attacks like worm-hole attack,malicious attack and black hole attack etc. Intrusion techniques are enhanced and that will use clusters and show how cluster can be used to isolate the attacks from the routing process. IDS can be composed of several components sensors which provide security events, a console to monitor events, alerts, control the sensors and center engine which records events logged by the sensor in a database. There are several ways to categorize the MANET depending on the type and location of the sensor and the methodology used by the engine to generate alerts.In many simple IDS implements all three components are combined in a single device or appliance.

The main challenge of this system is to find out the trusted nodes and its original position.so in this paper we discuss about the secure data transmission in the mobile network with verification of position by using NPV algorithm and CRT algorithm. The NPV performs majorly three operation in mobile network.

A. Securely determining own location.
B. Secure neighbor discovery
C. Neighbour position verification.

It mainly focus on to performs against several different colluding attacks.After NPV process the CRT algorithm will determine the huge data that can be divided by some give divisors. And the divided data is transmitted to the node via the various path and then finally collecting the divided data and merge that data and submit to the destination node.

II. SURVEY ON EXISTING SYSTEM:

Some of security data transmission using MANET are discussed below:
Yick,Mukherjee and Ghosal [1] has discussed the fault tolerance in Wireless Sensor Network(WSN). Fault tolerance is an important factor in WSN. Fault causes severe damage in a network, to reduce the fault in the network Negative Code Answering (NCA) Algorithm is proposed with the assistance of Mobile Agent (MA) techniques. Using NCA it identify the malicious and fault node in a network. The data aggregation is a method used to solve the overlap problems in data transmission.
S .Borasia,V. Raisinghani [2] has mainly discussed about the Congestion control. Congestion degrades overall channel capacity and increases packet lose rate. Any congestion control mechanism consists of congestion detection, congestion notification and rate adjustment mechanism.
The special difficulties in dealing with congestion due to their unique requirements and constraints. To find their common features, which may direct future research.
A.Rezai, M.K. Rafsanjani [3] have discussed mainly about the lossy communication medium in the WSN.The WSN are mainly affected by limited processing power and storage capacity, frequent topology change. Depending on the control policy the protocols

are divided into resource control vs traffic control. Despite the huge number of protocols are proposed in literature, congestion control in WSN remains challenging.

C. Luo and W.X. Xie [4] have solved the problem of Congestion, a novel algorithm for congestion avoidance and control, fuzzy active queue (FAQM), is proposed.

The simulation experiments show that FAQM can avoid and control the congestion, reduce the dropping rate of high priority packets and improve the whole network QOS performance.

D.J. Baker and J.Wieselthier [5] has proposed few updated data dissemination methods to refresh old replicas efficiently in mobile ad hoc network. In this presents a self-organizing, wireless mobile radio network for multimedia support.

G.Li,J.Li and B.Yu [6] in this they have discussed about the congestion not only leads to packet loss, but also increases delays and lowers network throughput with a lot of energy wastage due to retransmission.

They proposed a novel Weight Fairness Guaranteed Congestion Control protocol(WFCC).WFCC introduces a weighted fairness metric and gives its lower bound for the first time.

J. Broch, D.A. Maltz [7] have compared the performance of multi hop wireless ad hoc network routing protocols. The efficient routing protocols can provide significant benefits to mobile ad hoc network. In this they have present a logical survey on routing protocols and compare the performance of AODV, DSR and DSDV.

T.Camp,J. Boleng and V.Davies [8] has proposed the evaluation of a protocol for an ad hoc network. One of the main purpose of this paper is to investigate the impact on the mobility pattern.

The simulation results that illustrate the importance of choosing a mobility model in the simulation of an ad hoc network protocol. The performance results of an ad hoc network protocol drastically change as a result of changing the mobility model simulated.

G. Chatzimilioudis, D. Zeinalipour-Yazti and M.D. Dikaiakos [9] have proposed the evaluation is conducted to compare the proposed search algorithms with an algorithm based on R-tree Air Index. They develop a generalized search algorithm for continuous k-nearest neighbours based on Hilbert Curve Index in wireless data broadcast systems.

T-Y.Fu, W-C. Peng and W-C. Lee [10] has proposed the Spatial queries for extracting data from from wireless sensor network are important for many applications, such as environmental monitoring and military surveillance. These research works demonstrate that itinerary-based KNN query processing algorithm are able to achieve better energy efficiency.

III.   ATTACKS IN MANET

There are different types of attacks in MANET we are going to discuss briefly about few attacks BLACK- HOLE attack, GRAY-HOLE attack and JELLYFISH attack.

When this attacks occur in MANET which reduce the network efficiency and more packet losses, more energy consumption occur in the network. In the black hole attacks malicious node act as a black hole attack dropping all data packets from source to destination. It effectively separate the network it into two disconnected components. Gray hole attack which as its own characteristic behavior.

The most two common behavior in this are Node dependent attack and Time dependent attack. Jellyfish attack is somewhat different from Black whole and Grey hole attacks it will not blindly drop the packets instead of that it will reduce the flow control of mechanism.

IV.   APPROACH TOWARDS ATTACKS IN MANET.

To detect the black hole attack we have proposed AODV algorithm which is demand protocol and it establish and board cast route among the network with acknowledgement if the acknowledgement is received by destination it send request reply, otherwise it returns fake route.

After the detection of Black hole attack and to apply the Diffie - Hellman algorithm to transmit the date securely from source to destination.

This algorithm uses the asymmetric cryptographic to establish secure path between the source and destination.

Grey hole attack which is similar to black hole attack it also uses the AODV algorithm to detect the attackers from network. But in this tedious to find the original node and malicious node there will only slight changes between the nodes.

V. COMPARISON OF EXISTING WORKS

S.NO	TITLE	TECHNOLOGIES / TOOLS USED	ADVANTAGES	DISADVANTAGES
1.	Wireless sensor network survey.	Negative code Answering (NCA) with the assist of Mobile Agent.	These protocols have high packet delivery rate and it maintain vehicle information for better performance.	The existing algorithm is only efficient for low traffic situations. It fails when network topology rapidly changes.
2.	A review of congestion mechanisms for wireless sensor networks.	CODA, PCCP, FACC, Fusion and Siphon.	It reduces the storage space needed by the data collector and node can verify messages simultaneously.	Less network life time and High computational cost.
3.	Congestion control protocols in wireless sensor.	Using an effective transport protocol.	It helps to improve the routing in the network by reducing the size.	The ripple of re-clustering occur.
4.	Fuzzy AQM for congestion avoidance and control in sensor networks.	FAQM (Fuzzy Active Queue Management).	It is simple to create an effective Gaussian based models of the short path.	To complement the scientific literature by proposing us to set the parameters of the shortest path only considering the numbers of nodes.
5.	Lower bound of weighted fairness guaranteed congestion control protocol for WSNs.	WFCC (Weighted Fairness Guaranteed Congestion Control Protocol).	Router Free, Fault tolerance, cost.	Bandwidth Constraints, Energy constraints is more and High latency.
6.	A distributed algorithm for scheduling the activation of links in a self-organizing, mobile, radio network.	Self-organizing in wireless mobile radio network.	Reduce the energy consumption and decrease the hop count.	Scheduling for mobile sensors in sensors is more complex than that in sensing field.
7.	A performance comparison of multi-hop ad hoc network routing protocols.	MANET routing algorithm.	High packet delivery ratio, Increase Throughput and Low End to end delay.	High End to end delay and Low throughput.
8.	A survey of mobility for ad hoc network research.	Various mobility models in ad hoc networks.	These protocols are very scalable for medium to large size networks.	Vulnerable to malicious attacks.

VI. CONCLUSION

We have tried to categorize their different types of ad-hoc security attacks based on their characteristics. Our proposed methodology delete malicious node and repair such nodes and decrease the route discovery time. This could work very well in the presence of designated attacks. But there are many unanticipated and combined attacks that are still undiscovered. A lot of research are still in the process to find the threats.

REFERENCES

[1]   J. Yick, B. Mukherjee and D.Ghosal,   "Wireless sensor network survey", Computer Networks, Vol.52, No.12, pp.2292–2330, 2018.

[2]   S. Borasia and V. Raisinghani, "A review of congestion control mechanisms for wireless sensor networks", Springer Berlin Heidelberg Technology Systems and Management, pp.201–206, 2016.

[3]   A. Rezaei and M.K. Rafsanjani, "Congestion control protocols in wireless sensor networks: A survey", Journal of American Science, Vol.8, No.12, pp.772–777, 2015.

[4]   C. Luo and W.X. Xie, "Fuzzy AQM for congestion avoidance and control in sensor networks" , Chinese Journal of Electronics, Vol.42, No.4, pp.679–684, 2017.

[5]   G. Li, J. Li and B. Yu, "Lower bound of weighted fairness guaranteed congestion control protocol for WSNs", Proceedings of IEEE INFOCOM, pp.3046–3050, 2018.

[6]   D. J. Baker and J.Wieselthier, ``A distributed algorithm for scheduling the activation of links in a self-organizing, mobile, radio network,'' in Proc. ICC, 2015, pp. 2F6.1_2F6.5.

[7]   J. Broch, D. A. Maltz, D. B. Johnson, Y.-C. Hu, and J. Jetcheva, ``A performance comparison of multi-hop wireless ad hoc network routing protocols,''.

[8]   T. Camp, J. Boleng, and V. Davies, ``A survey of mobility models forad hoc network research, ''Wireless Commun. Mobile Comput., vol. 2,no. 5, pp. 483_502, 2017.

[9]   G. Chatzimilioudis, D. Zeinalipour-Yazti, W.-C. Lee, and M. D. Dikaiakos,``Continuous all k-nearest-neighbour querying in smartphone networks,'' inProc. IEEE MDM, Jul. 2016, pp. 79_88.

[10] T.-Y. Fu, W.-C. Peng, and W.-C. Lee, `` Parallelizing itinerary-based KNN query processing in wireless sensor networks, ''IEEE Trans. Knowl. DataEng., vol. 22, no. 5, pp. 711_729, May 2016.

[11] Lidong Zhou,Zygmunt J. Haas "Securing Ad Hoc Networks", IEEE network, special issue on network security ,pp 1 November/December , 2015.

[12] Taneja, K., & Patel, R. B "Mobile Ad hoc Networks: Challenges and Future", In Proceedings of National Conference on Challenges & Opportunities in Information Technology (COIT-2007), RIMT-IET, MandiGobindgarh, pp 1-2, March 2017.

[13] Yang, H., Luo, H., Ye, F., Lu, S., & Zhang, L "Security in mobile ad hoc networks: challenges and solutions", IEEE wireless communications, vol. 11(1), pp 38-47, 2017.

[14] de MoraisCordeiro, C., & Agrawal, D. P "Mobile ad hoc networking". Center for Distributed and Mobile Computing, ECECS, University of Cincinnati, OH-45221-0030, pp. 1-63, 2014.

[15] Wu, B., Wu, J., Fernandez, E. B., Ilyas, M., &Magliveras, S "Secure and efficient key management in mobile ad hoc networks", Journal of Network and Computer Applications, vol. 30(3), pp 937-954, 2013.

[16] Wu,J & Stojmenovic, I "Adhoc networks",Computer-IEEE Computer Society, vol. 37(2), pp. 29-31.

[17] Popat K.A., Priyanka Sharma, HardikMolia. "A Study of Routing Protocols for MANETs". In: Satapathy S., Bhatt Y., Joshi A., Mishra D. (eds) Proceedings of the International Congress on Information and Communication Technology. Advances in Intelligent Systems and Computing, vol. 438, pp. 1-3, 2017.

[18] Stephen E. Deering & David R. Cheriton "Multicast routing in datagram internetworks and extended LANs", Defense Advanced Research Projects Agency, vol. 8(2), pp. 86-106.

[19] Yoav Sasson David Cavin & Andre Schiper "Probabilistic Broadcast for Flooding in Wireless Mobile Ad hoc Networks", National Competence Center in Research on Mobile Information and Communication Systems(NCCR-MICS), a center supported by the Swiss National Science Foundation under grant 5005-67322, Pp.1-4 .

[20] Sze-Yao Ni, Yu-Chee Tseng, Yuh-Shyan Chen, and Jang-Ping Sheu "The broadcast storm problem in a mobile ad hoc network", In Proceedings of the Fifth Annual ACM/IEEE International Conference on Mobile Computing and Networking, pp. 151–162, Aug 2018.

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)