iJRASET
International Journal For Research in
Applied Science and Engineering Technology

INTERNATIONAL JOURNAL
FOR RESEARCH
IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 7 Issue: XII Month of publication: December 2019

DOI: http://doi.org/10.22214/ijraset.2019.12052

Review of Authentication Techniques for MANET using Security against Malicious Attack

Uday Shankar Choudhary[1], Dinesh Kumar Sahu[2]
[1, 2]Department of Computer Science & IT, SRK University Bhopal M.P., India

Abstract: The absence of centralized administration is really a major issue by that security is the major concern in Mobile Ad hoc Networks because of open environment of network. Due to dynamic topology, it is not easy to maintain strong connection in between sender and receiver. The MANET is the collection of mobile hosts that communicate with each other without any infrastructure. The security vulnerabilities of the routing protocols may be unprotected against attacks by the malicious nodes. The malicious attacks are maintained the integrity and absorbing all data packets in the network. Since the data packets do not reached the destination node on account of this attack, data loss will occur..

Keywords: Security, Malicious Attack, Routing, IDS.

I. INTRODUCTION

We talked about the issue of secure steering in Mobile Ad Hoc Networks and different issues required all the while. We some time ago thought about of the Intrusion Detection components anticipated in the writing for MANETs.

In the writing overview, we examined distinctive sorts of ways to deal with Intrusion Detection in MANETs. Separately of the techniques works best for an accepted kind of assault, for a particular situation. The vast majority of the issues function admirably for Intrusion Detection one-bounce away. There are not various scattered answers speaking Intrusion Detection where it counts.

In the following part, we talk about our way to deal with the issue of interruption discovery in MANETs as for arrangement number alteration assault and bundle dropping assault.

II. RELATED WORK

The few Intrusion Detection in MANETs applications as compared to other domains. Reported their experience in trying to automatically Past research in dealing with this problem can be described with the following approaches:

A. Method to ensure in inconsistency of permit Bout in portable specially appointed Network abuse Digital Signature [1]. They contemporaneous a gadget that is advantageous in interruption of empty assault in portable impromptu net is affirmation of computerized marks of association hubs by accepting hub therefore of each genuine hub inside the system contains the advanced mark of each extraordinary real hubs of same system.

B. Denial of Service Attack in AODV and intensifier; Acquaintance choices Withdrawal to style Detection Engine for Intrusion Detection System in Mobile Ad-hoc Network. Amid this work Denial of Service, assault is connected inside the system, confirms square measure gathered to style interruption location motor for painter Intrusion Detection System (IDS).

C. Countermeasures against Multicast Attacks on Enhanced-On Demand Multicast Routing Protocol in MANETs. This work focuses on raising the Secure Enhanced-On Demand Multicast Routing Protocol (EODMRP) to protect it against flooding and district assaults.

D. AN Attacks Analysis in versatile specially appointed systems: Modeling and Simulation. Amid this title blessing work is committed to check assaults and countermeasures in painter. Once a short prologue to what Manet's square measure and system security we tend to blessing a study of differed assaults in MANETs addressing come up short steering conventions.

III. OVERVIEW OF PROPOSED APPROACH

In Intrusion location framework (IDS) , each hub needs two extra little estimated tables; one to keep last-bundle grouping numbers for the last parcel sent to each hub and the other to keep last-parcel arrangement numbers for the last parcel gotten from each hub (from hub through hub). The sender communicates the RREQ bundle to its neighbors. At the point when this RREQ touch the objective, it will select a RREP to the source, and this RREP will contain the last-parcel arrangement numbers set up from this source.

A. Classification

Techniques for Security against Malicious Attack

There are a few basic methods to identify vindictive hubs in a system however these have some essential imperfections which are talked about

Link Frequency Analysis. Investigation of the connection recurrence is a straightforward technique to identify a noxious in a system. Unusually high recurrence of a connection could recommend that it can be a malevolent tricking movement into it.

Trust Based Model. Another huge technique to recognize malevolent action of atis by the utilization of trust data. Hubs can screen the conduct of their neighbor and rate them. Accepting that a pernicious drops every one of the bundles it gets as in dark openings, a vindictive in such a framework ought to have the minimum trust level and can be effectively dispensed with.

Dim gap assaults is a vigorous assault kind that bring about dropping of messages. Hostile hub introductory consents to forward bundles therefore} neglects to attempt to so. Toward the begin the hub acts legitimately and replays genuine RREP messages to hubs that start RREQ message. Along these lines, it assumes control over the causation parcels.

Black Hole Attacks contrasted with Gray Hole Attacks is that malevolent hubs never send genuine control messages at first. Toward do a dark gap event, evil hub sits tight for neighboring hubs to send RREQ messages. At the point when the devilish hub gathers, a RREQ message, without review its steering table, specifically sends a false RREP message giving a course to focus over itself, exchange a high grouping number to settle in the directing table of the casualty hub, before different hubs send a genuine one.

IV. RESULTS/ DISCUSSION

In this chart the execution examination of aggressor misconduct is assessed regarding misfortune rate. The assailant misfortune rate is consistently debases with deference of time and most minimal is 14% toward the finish of reproduction

V. CONCLUSION / FUTURE WORK

The damage will be serious if malicious node in a network working as an attacker node absorbs all data packets delivered through them. In this researchwe proposed a novel Intrusion Detection System (IDS), neighbor based against malicious attack and measure the network performance after applying IDS scheme and malicious attack. The comparison of security scheme is applied on packet dropping attack and observe that the proposed security based scheme is provides better results in dynamic network. The routing misbehavior is evaluated negligible in dynamic network. The simulated scenario of normal, malicious and proposed security scheme against attacks is simulated in network simulator 2 (ns-2) and measured the packet loss in the presence of packet dropping attack and in presence of proposed IDS. The security scheme is improves the network performance and provides the reliable communication among the mobile nodes in the

The energy efficient utilization of node is also the important issue in MANET. In Future we also work out on effect of attack on Node Energy, location based routing and Multicast routing protocols.

REFERENCES

[1] W. Li, A. Joshi, and T. Finin, “Coping with node misbehaviors in ad hoc networks: A multi-dimensional trust management approach,” in Proceedings of the Eleventeenth International Conference on Mobile Data Management, 2010. MDM ’10. IEEE Computer Society, May 2010.

[2] J. Cho, A. Swami, and I. Chen, “A survey on trust management for mobile ad hoc networks,” Communications Surveys Tutorials, IEEE, vol. PP, no. 99, pp. 1 –22, 2010.

[3] G. Theodorakopoulos and J. S. Baras, “Trust evaluation in ad-hoc networks,” in WiSe ’04: Proceedings of the 3rd ACM workshop on Wireless security. New York, NY, USA: ACM, 2013, pp. 1–10.

[4] W. Li, J. Parker, and A. Joshi, “Security through collaboration and trust in manets,” ACM/Springer Mobile Networks and Applications (MONET), pp. 1–11, 2014 (Online First).

[5] A. Patwardhan, A. Joshi, T. Finin, and Y. Yesha, “A data intensive reputation management scheme for vehicular ad hoc networks,” in Proceedings of the 3rd Annual International Conference on Mobile and Ubiquitous Systems - Workshops, Mobiquitous ’06., July 2015, pp. 1–8.

[6] P. Michiardi and R. Molva, “Core: a collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks,” in Proceedings of the IFIP TC6/TC11 Sixth Joint Working Conference on Communications and Multimedia Security. Deventer, The Netherlands, The Netherlands: Kluwer, B.V., 2015, pp. 107–121.

[7] Y. Zhang and W. Lee, “Intrusion detection in wireless ad-hoc networks,” in MobiCom ’00: Proceedings of the 6th annual international conference on Mobile computing and networking. New York, NY, USA: ACM, 2015, pp. 275–283.

[8] S. Marti, T. J. Giuli, K. Lai, and M. Baker, “Mitigating routing misbehavior in mobile ad hoc networks,” in MobiCom ’00: Proceedings of the 6th annual international conference on Mobile computing and networking. New York, NY, USA: ACM, 2015, pp. 255–265.

[9] S. Buchegger and J.-Y. Le Boudec, “Performance analysis of the confidant protocol,” in MobiHoc ’02: Proceedings of the 3rd ACM international symposium on Mobile ad hoc networking & computing. New York, NY, USA: ACM, 2016, pp. 226–236.

[10] Y.-A. Huang and W. Lee, “A cooperative intrusion detection system for ad hoc networks,” in SASN ’03: Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks. New York, NY, USA: ACM, 2018, pp. 135–147.

[11] S. Buchegger and J.-Y. Le Boudee, “Self-policing mobile ad hoc networks by reputation systems,” IEEE Communications Magazine, vol. 43, no. 7, pp. 101–107, July 2018.

[12] P.-W. Yau and C. J. Mitchell, “Security vulnerabilities in ad hoc networks,” in Proceedings of the 7th International Symposium on Communication Theory and Applications, 2017, pp. 99–104.

[13] Edgar Osuna, Robert Freund, and Federico Girosi. Training Support Vector Machines: an Application to Face Detection. In CVPR ’97: Proceedings of the 1997 Conference on Computer Vision and Pattern Recognition (CVPR ’97), page 130, Washington, DC, USA, 1997. IEEE Computer Society.

[14] Cheng Soon Ong, Alexander J. Smola, and Robert C. Williamson. Learning the Kernel with Hyperkernels. Journal of Machine Learning Research, 3, 2003.

[15] Mahesh Pal and Paul M Mather. Support Vector Classifiers for Land Cover Classification, 2003. Map India Conference.

[16] George Quievryn. Mutplus - glossary.

[17] Florian Steinke, Sch¨olkopf, and V. Blanz. Support Vector Machines for 3D Shape Processing. Computer Graphics Forum (Proc. EUROGRAPHICS), 24(3), August 2005.

[18] O. Teytaud and R. Jalam. Kernel-based text categorization, 2001.

[19] Vladimir N. Vapnik. The nature of statistical learning theory. Springer-Verlag New York, Inc., New York, NY, USA, 1995.

[20] Larry L. Peterson and Bruce S. Davie, “Computer Networks - A Systems Approach”. San Francisco, Morgan Kaufmann Publishers Inc.

[21] Chia-Chen, H., H. Chan, et al. 2008, Mobility Pattern Aware Routing for Heterogeneous Vehicular Networks. IEEE Wireless Communications and Networking Conference, WCNC 2008.

[22] Abdulrahman H. Altalhi Golden G. Richard, III “Load-Balanced Routing through Virtual Paths:Highly Adaptive and Efficient Routing Scheme for Ad Hoc Wireless Networks”,IEEE,2004

[23] J. Broch, D.A. Maltz, D.B. Johnson, Y. Hu and 1.Jetcheva, "A Performance Comparison of Multi-hop Wireless Ad Hoc Network Routing Protocols," in Proceedings of ACM MOBICOM'98, Dallas, Texas, USA, October 1998..