International Journal of Emerging Research in Management &Technology ISSN: 2278-9359 (Volume-7, Issue-1)

Research Article | **January 2018**

DDoS Attacks Detection and Prevention in Mobile Adhoc Network: A Survey

Ranjana Kumari*, Achint Chugh

Department of ECE, MIT, RGPV, Bhopal, Madhya Pradesh, India

ranjanaguddi123@gmail.com, achintchugh@gmail.com

Abstract—

Ad-hoc system is a gathering of wireless movable nodes enthusiastically creating a momentary network lacking the use of any core-existing centralized administration or network infrastructure. MANET has some limitations owing to infrastructure, mobility, capabilities of mobile nodes or due to system as a whole. Limitations due to infrastructure or system, Broadcast nature of communications, frequent disconnections / partitions, Limited bandwidth, packet loss due to transmission error, variable capacity links. Cooperative procedures, Exposed medium, dynamically varying system topology, inadequacy of centralized monitoring, Nonexistence of clear line of resistance. There is no layered security in MANETs like in wired network. Data packets routed between a sender node (source) and a receiver node (destination) of a MANET often traverse along a path spanning multiple links, which is known as the multihop path. The paper provides survey to DDoS attacks prevention and detection methods.

Keywords— MANET, Attacks, Routing, Node, Security, DDoS

I. INTRODUCTION

In MANET[1] the mobile wireless network is not rely on any existed network. It is a combination of several wireless nodes that can build a network randomly. The study and growth of mobile devices and 802.11[2] Wi-Fi wireless networks is on demand topic of research in MANE. Ad-hoc network doesn't depend on any central administration or stable infrastructure such as base. While nodes are moving in the network they interchange the information to each other and may continue to move here and there and so the network must be prepared. Mobile devices are not having the centralized control, therefore they are free to move, and hence the topology of such network changes expeditiously. In the mobile Adhoc system, a number of influences such as physical obstacles movement, unwanted noise, and climate circumstances contribute to the trouble of precisely forming the actions of the lifetime of a link among two mobile nodes. The excellence of service must fulfil source end to destination end data packet transfer without packet loss. Data packets routed between a sender node (source) and a receiver node (destination) of a MANET often traverse along a path spanning multiple links, which is known as the multihop path[3].

While nodes are moving in the network they interchange the information to each other and may continue to move here and there and so the network must be prepared. Digital information are growing using the networks of mobile devices anywhere at any time and becoming the need of today. Without using some static structural support the info is transferring in the setup of mobile devices. This type of networks is called as ad – hoc network. To set up the network for the nodes for short period of time is objective of the of ad-hoc network. MANET is a setup which workings on idea of having network without any static infrastructure. Such network consists of mobile nodes which are free to move. They come together for a span of time for give and take process means to receive and give the information in return. All information is used by each device, can be assumed as producers and consumers in an ad-hoc network. While nodes are moving in the network they interchange the information[4] to each other and may continue to move here and there and so the network must be prepared. Ad hoc setup reduces the requirement of static infrastructure and install the speed.

To accomplish availability and reliability network routing protocols should be prevailing compared to distributed type of denial of service security attacks. The trustworthiness of distributing data packets from end to

© www.ermt.net All Rights Reserved

end using multi-hop intermediary nodes is a noteworthy problem in the mobile Adhoc network. Due to the intrinsically self-motivated nature of the mobile system network layout, the prevailing data routes cannot be secure. Determination of data link letdown, info safety, recognition of malicious node and protected information transmission within MANET is a significant tasks in any mobile network. The paper emphases on the following problem: Detection, prevention and correction of distributed denial of service attack in multipath mobile Adhoc network and to increase performance and trustworthiness of mobile Adhoc network under DDoS malicious attack with secure data transmission and routing.

The main aim is to notice secure route of the mobile network, to improve the data delivery ration and performance of MANET, to select best route for secure data transmission. The trustworthiness of distributing data packets from end to end using multi-hop intermediary nodes is a noteworthy problem in the mobile Adhoc network. Detection of DDoS attacks[1], info security[5], detection of DDoS malicious node and secure information transmission in a MANET is an important tasks in any mobile network.

The objectives are to detect distributed denial of service attack in MANET, to provide prevention of MANET from distributed denial of service attack,

The rest of the paper is organized as follows.

Section 2 represents background related to DDoS prediction, detection and failure. Section 3 provides literature survey. Section 4 provides the problem identification of survey. Section 5 concludes the paper with a summary of the work and discussion of future research directions.

II. BACKGROUND

The study and growth of mobile devices and 802.11 Wi-Fi wireless networks is on demand topic of research in manet. As per the style of operation[6] ad-hoc network are basically works on peer to peer communication among many node mobile wireless network. Some of the applications of MANET are: Military drill or police routine, Disaster relief operations, Mine site operations, Urgent meetings, Robot data acquirement, Packet radio network, Commercial application like third generation network. MANET's having number of node demands high quality of processing power, high bandwidth and memory to provide definite routing information, though induces traffic overhead in the network. In this the information of data are circulates in the network. MANET has some limitations owing to infrastructure, mobility, capabilities of mobile nodes or due to system as a whole. Limitations due to infrastructure or system, Broadcast nature of communications, Frequent disconnections / partitions, Limited bandwidth, Packet loss due to transmission error, Variable capacity links. As when nodes communicate to each other for transferring the information consumes more battery power in return. The thought of Ad-hoc networking usually termed as infrastructure less networking [7]. In this type of the network, mobile devices functions as router and as host. They forward the information packet to other devices even if they are not in direct range of transmission. Limitations due to mobility, Dynamically changing topologies, Lack of mobility awareness by system/applications, Tedious identification mechanism / IP address assignment, Limitations due to capabilities of mobile nodes, Short battery life. Limited capacities – memory, radio range, application softwares. self-configured and infrastructure less network of mobile nodes is called as MANET. Ad-hoc is Latin word which reflects as "for this and only for this" [7]. Every mobile node is free to move in any ways and can change their link at any time.

While nodes are moving in the network they interchange the information to each other and may continue to move here and there and so the network must be prepared. Digital information are growing using the networks of mobile devices anywhere at any time and becoming the need of today. Without using some static structural support the info is transferring in the setup of mobile devices. This type of networks is called as ad – hoc network. To set up the network for the nodes for short period of time is objective of the of ad-hoc network. MANET is a setup which workings on idea of having network without any static infrastructure. Such network consists of mobile nodes which are free to move. They come together for a span of time for give and take process means to receive and give the information in return. All information is used by each device, can be assumed as producers and consumers in an ad-hoc network. While nodes are moving in the network they interchange the information to each other and may continue to move here and there and so the network must be prepared. Ad hoc setup reduces the requirement of static infrastructure and install the speed.

MANETs are highly affected to attack than wired network[9]. Following are the reasons: Mobile devices are not having the centralized control, therefore they are free to move, and hence the topology of such

© www.ermt.net All Rights Reserved

network changes expeditiously. Open medium, Dynamically changing network topology, Cooperative algorithms, Inadequacy of centralized monitoring, Lack of clear line of defense. There is no layered security in MANETs like in wired network. Some of the advantages of MANET are to provide the access of details and assistance regardless of geographic position[10], network built up at any fraction of time and place, and such network performs without any infrastructure. The different disadvantages of MANET are resources are limited, restricted to physical security, authorization facilities are deficit, hard to detect malicious nodes.

The distributed mobile nodes create links to form the MANET, which may include mischievous and selfish nodes[11]. Developing the trust based system is very challenging problem in MANET. In order to filter out misbehaving nodes the system proposes a model which help in secure route discovery, data transmission and report to the MANET about any mischievous node. And also find secure data path for secure data transmission. The proposed system estimate the secure value of each node using timestamp of the operation. Then to select a protected track[11] for message forwarding to identify the damaged and malicious nodes which are supposed to launch network letdown.

AODV utilize the source routes where packet travels according to obtained source route from the route cache itself or by finding through the flooding in the network. The concepts dynamic source routing is based on the source routing which means the initiator of the packet provides an orderly list of nodes according to which packet traverses in the network. The key note this routing pattern is that intermediate nodes need not to track the information of the routing through which packet will traverse in the network as source node already has a decision regarding the routes. All aspects of protocol operate entirely on demand .

A DoS attack prevents users from accessing the services. In DoS attack node sends excessive messages to block the services. Distributive denial of service (DDoS) makes the network resources unavailable. In DDoS attacks the incoming traffic flooding the nodes from many different sources.

In the mobile Adhoc system, a number of effects such as physical obstacles movement, unwanted noise, and climate circumstances contribute to the trouble of precisely forming the actions of the link failure of a link among two mobile nodes. To accomplish availability and reliability network routing protocols should be prevailing compared to distributed denial of service attacks. Due to the intrinsically self-motivated nature of the mobile network topology, the existing links are recurrently damaged, and fresh links are often recognized. Detection and correction of attacks to increase performance and trustworthiness of mobile Adhoc network using dynamic source routing under malicious attack with secure routing and data transmission. Recognition of distributed denial of service node data Security and within a MANET is an imperative tasks in any network. The excellence of service must fulfil source end to destination end data packet transfer without packet loss. To improve the data delivery ration and performance of MANET and also detect and correct attacks is the main problem in MANET. Mobile Adhoc network needs safety and consistency of data packets. Real time applications in MANET require certain QoS[15] features, such as minimal source end to destination end data packet delay and acceptable data loss. Determination of data security, detection of malicious node and secure information transmission within a MANET is an significant tasks in any mobile network. Detection of secure route of mobile nodes with the help of routing info is also problematic in an ad hoc network due to its real time altering topology. Data packets routed between a sender node (source) and a receiver node (destination) of a MANET often traverse along a path spanning multiple links, which is known as the multihop path. The proposed protocol discover the best route and if original link is breakdown then new secure node is established and information is transferred from newly created mobile route. The objective is to detect secure route of the mobile network, to improve the data delivery ration and performance of MANET, to select best route for secure data transmission.

III. LITERATURE SURVEY

At present-day, more and more compound system network traffic is designated by using a traffic prototypical in network traffic capacity. Low-rate denial of service (LDoS)[1] attacks send periodic pulse sequences with relative low rate to form aggregation flows at the victim end. LDoS attack flows have the characteristics of low average rate and great concealment. Low-rate Denial of Service (LDoS) attack is a new type of DoS attack. LDoS attacks exhibit a periodic pulse sequence, which can be expressed in a triple of attack period T, attack duration L, and attack rate R. LDoS attacks send attack packets periodically in a short time interval. The network multifractal must be disrupted when LDoS attacks are launched suddenly.

© www.ermt.net All Rights Reserved

It is tough to identify LDoS attack streams from standard traffic due to low rate property. Although the LDoS attack movements are very minor, it will inescapably lead to the variation of multifractal appearances of network traffic. LDoS attacks effort to contradict bandwidth to TCP flows while conveyance at satisfactorily low average rate to get away detection by counter-DoS mechanisms. The LDoS attacks may keep damaging the victim for a long time without being detected. DDoS oriented detection methods are no longer suitable for the detection of LDoS attacks. The investigators found that the self-similar prototypical with its single scaling parameter is not adequate as a manifold scaling on fine timescales.

The procedure of multifractal detrended oscillation analysis (MF-DFA)[12] is used to discover the modification in relations of multifractal characteristics over a small scale of network traffic due to LDoS attacks. A new approach of detecting LDoS attacks is proposed by monitoring the abrupt change of Holder exponent through wavelet analysis. The DFA procedure is extensively used in authenticating the scale characteristic of monofractal and in perceiving the long-range connection of noisy nonstationary sequences. By using the MF-DFA algorithm, researchers can achieve the multifractal spectrum easily and analyze the multifractal characteristic of nonstationary sequences effectively.

Yu[13] proposed a collaborative approach of defense against periodic shrew DDoS attacks in the frequency domain. This approach detected shrew DDoS attacks using the frequency-domain characteristics from the autocorrelation sequence of Internet traffic streams.

Barford introduced the wavelet processing idea in detecting LDoS attacks by using the discrete wavelet transform (DWT)[14] technology. This method transforms network traffic into high, middle, and low frequency components for the purpose of finding the attack traffic.

Wu presented an LDoS attack detection method using the technique of one step prediction Kalman filtering. This method explored the characteristics of network traffic observed at the victim end when the attack started. The error between one step prediction and the optimal estimation is used as the basis for detection.

Recommendation Based Trust Model with an Effective Defence Scheme for MANETs. It provides recommendation based trust model with a defence scheme, which utilises clustering technique to dynamically filter out attacks related to dishonest recommendations between certain time based on number of interactions, compatibility of information and closeness between the nodes. It only detect bad mounting attack. It does not provide prevention and detection from DDoS based attacks. Mitigating the Attacks on Recommendation Trust Model for Mobile Ad Hoc Networks. This paper provides information about recommendation based trust model for MANET. It successfully provides details and differentiated the honest and dishonest recommendations. This algorithm will not work on DDoS based attacks.

Preventing Malicious Node[15] and Provide Secure Routing In Manet. This paper provides SIEVE, a fully distributed technique to identify malicious nodes. SIEVE is very accurate and robustness under several attack scenarios and deceiving actions. The techniques adopted for the identification and the following removal of malicious nodes clearly require a joint and careful design to optimize the overall performance.

A Novel Hybrid Trust Management Framework for MANETs. To design a robust trust management framework. A hybrid trust management framework (HTMF) to construct trust environment for MANETs. The limitations is it will not work on selective misbehave attack and time attacks.

IV. PROBLEM IDENTIFICATION

To accomplish availability and reliability network routing protocols should be prevailing compared to distributed type of denial of service security attacks. The trustworthiness of distributing data packets from end to end using multi-hop intermediary nodes is a noteworthy problem in the mobile Adhoc network.

In the mobile Adhoc system, a number of effects such as physical obstacles movement, unwanted noise, and climate circumstances contribute to the trouble of precisely forming the actions of the link failure of a link among two mobile nodes. To achieve reliability and availability, routing protocols should be powerful against malicious attacks. Due to the intrinsically self-motivated nature of the mobile network topology, the existing links are recurrently damaged, and fresh links are often recognized. Detection and correction of attacks to increase performance and trustworthiness of mobile Adhoc network using dynamic source routing under malicious attack with secure routing and data transmission. The excellence of service must fulfil source end to destination end data packet transfer without packet loss. To improve the data delivery ration and performance of MANET and also detect and correct attacks is the main problem in MANET. Mobile Adhoc network needs

© www.ermt.net All Rights Reserved

safety and consistency of data packets. Real time applications in MANET require certain QoS features, such as minimal end-to-end packet delay and acceptable data loss. Detection of secure route of mobile nodes with the help of routing info is also problematic in an ad hoc network due to its real time altering topology. Data packets routed between a sender node (source) and a receiver node (destination) of a MANET often traverse along a path spanning multiple links, which is known as the multihop path.

V. CONCLUSIONS

Ad-hoc network doesn't rest on any principal supervision or stable infrastructure such as base. The study and growth of mobile devices and 802.11 Wi-Fi wireless networks is on demand topic of research in MANET. Real time applications in MANET require certain QoS features, such as minimal end to end info packet interval and acceptable data loss. AODV set of rules is a sensible protocol in wireless mobile ad-hoc network. The excellence of service must fulfil source end to destination end data packet transfer without packet loss. The trustworthiness of distributing data packets from end to end by means of multi-system intermediary nodes is a remarkable difficulty in the mobile Adhoc network. Owing to the innately enthusiastic nature of the movable system topology, the prevailing routes cannot be secure. MANET network using AODV under distributed denial of service malicious attack with secure routing and data transmission. The paper represented security from the DDoS attack.

REFERENCES

[1] Zhijun Wu, Liyuan Zhang, and Meng Yue , Low-Rate DoS Attacks Detection Based on Network Multifractal, IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 13, NO. 5, SEPTEMBER/OCTOBER 2016, pp-559-567

[2] S. T. Zargar, J. Joshi, and D. Tipper, "A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks," IEEE Commun. Surveys Tuts., vol. 15, no. 4, pp. 2046–2069, Fourth Quarter 2013.

[3] David A. Maltz, "On demand routing in multi-hop wireless mobile ad-hoc network" CMU-CS 01-130, PhD. Desertion, School of computer science Carnegie Mellon University, Pittsburgh PA- 2001.

[4] Josh Broch ,David A. Maltz , David B Jhonson, Yih-chun hee, Jorjeta Jatchene, " A Performance Comparison of Multi-Hop Wireless Ad-hoc Network Routing Protocol", Computer Science Department Carnegie Mellon University Pittsburg PA 15213, Available at http : //www . monarch .cs.cmu.edu/

[5] Antesar M. Shabut, Keshav P. Dahal, Sanat Kumar Bista, and Irfan U. Awan, Recommendation Based Trust Model with an Effective Defence Scheme for MANETs IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 14, NO. 10, OCTOBER 2015, pp-2101-2114

[6] Hongmei Deng, Wei Li, and Dharma P. Agrawal, Routing Security in Wireless Ad Hoc Networks, IEEE 2002, pp-433-445

[7] U. Venkanna, R. Leela Velusamy, Mitigating the Attacks on Recommendation Trust Model for Mobile Ad Hoc Networks, IEEE 2015, pp 223-234

[8] Wenjia Li, Anupam Joshi, Tim Finin, CAST: Context-Aware Security and Trust Framework for Mobile Ad-hoc Networks Using Policies, IEEE 2010, pp-188-201

[9] Charlos De Cordeiro and Dharma P. Agarwal " Mobile ad-hoc networking",OBR Research Centre for Distributed and Mobile Computing,ECECS,University of Cicinnati –USA.

[10] Amit N Thakre ,Mrs M.Y.Joshi "Performance Analysis of AODV & DSR routing Protocol in Mobile ad-hoc network", IJCA special Issue on "mobile ad-hoc network"MANETs 2010.

[11] Pravin Ghosekar, HOD, Computer Department, Dhanwante National college, Nagpur,(MS),Girish Kathkar, HOD,Department of computer science ACS College Karodi, dist Nagpur (MS), Dr.Pradip Ghorpode Shivaji Mahavidyalaya, Gadchiroli (MS) India," Mobile Ad-hoc networking: impartaive and challenges,IJCA Special Issue,"Mobile Ad-hoc Network" MANETs 2010.

[12] Sukhpreet Kour Mtech.,Sukhpreet Kour(Assistant professor of CSE Department),chandan kumar (Ph.D candidate),"An overview of mobile ad-hoc network: Application challenges and comparison of Routing Protocols", IOSR Journal of Computer Engineering (IOsR-JCE),e-ISSN:2278- 0661,p-ISSN :2278-8727 volume 11,issue 5(May-JUNE .2013).pp 07-11

© www.ermt.net All Rights Reserved

[13] Rajesh H Danda ,Mitesh B Nakrani ,Chirag R .Patel ,CU Shah College of engineering and technology, wadhwan Gujrat, India , "Analysis of various routing Algorithm for Mobile Ad-hoc network", IJTCSE International Journal of Technology in Computer Science & Engineering Volume 1(2),June 14,pp 27-32, Available on http://www.ijtcse.com.

[14] Geetha Jayakumar and Gopinath Ganapathy,"Performance Comparison of Mobile Ad-hoc network Routing Protocol "International Journal of Computer Science and Network security", (IJCSNS), Vol. 7 No.11 pp 77-84 November 2007.

[15] National Science Foundation Research priorities in wireless and Mobile communications and Networking: Report of workshop held March 24-26,1997,Airlie House,Virginia.Available at http://www.cise.nsf.gov/anir/ww/html

© www.ermt.net All Rights Reserved