ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 8, Issue 12, June 2019

A Survey - Packet Loss Avoidance and Fine Grained Analysis in Mobile Adhoc Network

Aashish Kumar Mishra

Abstract—Mobile Ad-Hoc Network (MANET) is associate infrastructure less arrangement of mobile nodes which will randomly modification their geographic locations such these networks have dynamic topologies and random mobility with forced resources. Numerous inherent limitations like totally distributed architecture and constantly varying topology, make MANET as vulnerable to a number of attacks by mischievous nodes. Present trust-based systems fail to internment the real primary origins of an adversative event which may leads to several false positives through which valid nodes are acknowledged malicious and to little detection rates for malevolent nodes.Comprehensive examination and analysis of data packet are necessary to discover the actual reason of the packet loss. Without fine-grained analysis the network may treat normal nodes as malicious and can disconnect from communication. It can degrade the network performance and malicious nodes remain undetected. The paper represents the survey to packet loss avoidance methods in mobile adhoc network. It also represents fine grained analysis of packet data.

Keywords: **MANET, Packet Loss Analysis, Malicious node, FGA, PDR.**

I. INTRODUCTION

Ad hoc Wireless network does not have some collective server but is a novel distributed, almost autonomous of any pre-established arrangement system. A MANET [1] is a gathering of moving wireless nodes that can enthusiastically be set up anytime and anywhere without using any pre-existing network arrangement. The nodes in the network are themselves responsible for routing the packets from the source to the destination. It is a widely used routing protocol for mobile ad hoc networks (MANETs). These nodes are also responsible to make the transfer of packets secure. Ad hoc On-Demand Distance Vector (AODV). AODV[2] is, as the name suggests, a distancevectorrouting protocol. It is also used for other wireless ad-hoc networks. AODV is an approachable routing set of rules i.e.it founds a source to an endpoint only on request. In dissimilarity, the widely used routing protocols of the WWW are proactive, i.e. they find routing track autonomously of the usage of the paths.

The main characteristic of the Adhoc network is dynamic topology. In this, nodes changes its position often and these nodes have to adapt for the network topology change. Each node should maintain some CPU capacity, storage capacity, battery power and bandwidth. So that routing protocol try to minimize the traffic in packet transmission.

Normal routing protocol in fixed network does not show the same performance in MANET. In this, if the two mobile nodes are not in the same transmission range, message communication between the nodes can be done through the intermediate node. This node can also change their position, so that network should adapt to the topology change. Since there is no existing communication infrastructure, adhoc networks cannot rely on specialized routers for path discovery and routing. Therefore, nodes in such a network expected to cooperatively to establish routes instantly.Numerous inherent limitations, like totally distributed architecture and constantly varying topology, make MANET as vulnerable to a number of attacks by mischievous nodes. In MANET all nodes cooperation is necessary in order to make sure an appropriate functionality.

Some of examples of node attacks are: (i)a node may drops data packets because of malicious behaviour; (ii)a node doesn't take part in routing procedures[3] in order to protect its energy and (iii) a node make available fake routing information to other nodes in order to interrupt the network. To isolate and identify nodes which are non-cooperative in MANETs, an array of trust-based safety systems have been suggested. According to MANETs, trust can be well-defined as to what amount a node can accomplish the anticipations of another node. In trust-based systems, each node within the network be able to manage a sovereign trust table to store and compute the trust values [4] of former nodes. Routing choices are then constructed on such calculated trust values.

Present trust-based systems fail to internment the real primary origins of an adversative event which may leads to several false positives through which valid nodes are acknowledged malicious and to little detection rates for malevolent nodes. The motive for such deficiencies is that individual's trust-based safety systems assume that packet damages only get up due to mischievous actions by disobedient nodes. Conversely, packet damages in MANETs possibly will rise because of other adversative events, like congestion, wireless link transmission errors, and mobility. Deprived of a fine-grained investigation of packet damages in the trust building procedure, traditional systems may outcome in inaccurate trust assessments, specifically below high node mobility and high data rate. The rest of the paper is organized as follows.

Section 2 represents security issues, fine grained analysis and packet loss avoidance related background. Section 3 provides literature survey. Section 4 concludes the paper with a summary of the work and discussion of future research directions.

Manuscript received: 25 May 2019
Manuscript received in revised form: 21 June 2019
Manuscript accepted: 06 July 2019
Manuscript Available online: 10 July 2019

DOI:10.17605/OSF.IO/GS9FK

II. SECURITY ISSUES, FGA, PACKET LOSS

The connectivity of mobile nodes over a wireless link in MANETS that is multi hop in nature powerfully depends on the actual fact that ensures cooperation among the nodes within the network. Since network layer protocols forms property from one hop neighbors to any or all different nodes in MANET, the peace of mind of cooperation among nodes is needed. The attacks in MANETS are classified into two major categories, particularly passive attacks and active attacks, consistent with the attack suggests that [2]. Passive attacks are those, launched by the adversaries entirely to snoop the info changed within the network. These adversaries in any method don’t disturb the operation of the network. Such attacks identification becomes very tough since network itself doesn't affect and that they will reduced by exploitation powerful cryptography techniques. But a vigorous attack tries to change or destroy the data that's being changed, thereby heavy the traditional practicality of the network.

Passive attacks are enumerated as overhearing, traffic investigation, and traffic observing. Active attacks include data revelation, wormhole, black hole, resource consumption, gray hole, routing attacks and others include modification, jamming, impersonating, message replay and DoS. Such attacks is prevented by exploitation powerful cryptography techniques and firewalls. Internal attacks are launched by the compromised nodes inside the network. This node tries to gather security data and may access the protected rights of the network. Since the compromised node is an authorized one within the network, it's terribly tough to spot the internal attacks. Each security framework must give a heap of security capacities that can guarantee the mystery of the framework.

MANETs are much more vulnerable to attack than wired network. This is because of the following reason:-

Open medium- Eavesdropping is more easier than in wired network.

Dynamic changing network topology-Mobile node comes and goes from the network, thereby allowing any malicious node to join the network without being detected

Lack of centralized monitoring– Absence of any centralized infrastructure prohibits any monitoring agent in the system

Battery constraints: Devices used in these wireless networks has constraints on the power source in mandate to conserve movability, size and weightiness of the device.

Maximum present trust-based security arrangements for MANETs consider packet loss as a sign of probable attacks by means of malicious nodes. The packet loss possible reasons may be node mobility, queue overflow and interference. Recognizing the actual fundamental reason of a packet loss event is essential for any security scheme.

The actual reason to find packet loss and malicious node fine grained analysis is necessary. Because detection of innocent nodes as malicious nodes and without fine grained analysis the performance of MANET may degrade. And also malicious nodes may remain undetected without fine grained analysis. Consequently, methodologies are necessary that can appropriately recognize the main reason for packet losses and can respond accordingly.

Packet loss detection, reaction and report to the MANET is a significant factor of any widespread safety solution. Comprehensive examination and analysis of data packet are necessary to discover the actual reason of the packet loss. Before isolating mischievous nodes from the route in trust-based safety arrangements, a FGA of packet is essential to avoid false positives. Short of FGA of packet investigation, the performance of primary safety systems may cut down, resultant in the penalty of not guilty nodes and discontinuation of portions of the system network, although real malicious nodes remain undetected. Therefore, current MANET trust-based schemes need to be extended with approaches able to perform an accurate identification of packet losses, in view of run-time network circumstances to distinguish correctly mischievous nodes.

III. LITERATURE SURVEY

Elisa Bertino et. al. [5] represents a system that is capable to appropriately recognize malicious nodes, by applying network parameters to decide whether packet losses are because to node mobility or queue overflows in MANETs. The author proposed FGA system for packet loss and the improvement of a wide-ranging trust model for mischievous node isolation and identification. The suggested FGA system is estimated in relations of performance metrics and efficiency under dissimilar network configurations and parameters. The experimental outcomes show that the proposed trust system accomplishes a noteworthy lessening in false positives degree and a rise in the rate of recognition of accurately mischievous nodes compared with normal non-FGA systems. FGA system inspects the reasons of data packet losses and provides information to the network about most possible reason of packet losses.

The proposed model first recognizes the main parameters for investigating the reason of packet losses in dissimilar aspects. The FGA system applied a number of dissimilar parameters like MAC layer data, queue data, and rate of link variations to summary the associations between nodes and nodes' neighbourhoods. The intention for applying local information for each node is to accomplish more perfect information and observation of network. Even though global information possibly will in some circumstances make available appropriate information, it is probable that false information delivered by the mischievous node can evade the safety mechanisms. In addition, as the FGA system necessitates information about the node neighbourhood, each node applied its personal local data to take a more informed result. The author present a method that is capable to appropriately recognize malevolent nodes, with the help of network parameters to conclude whether packet losses are because of queue overflows or node mobility in Adhoc. The authors proposed method for data packet loss and the improvement of a widespread trust system for malicious node identification and isolation. The proposed Fine-grained analysis method is estimated in terms of effectiveness and performance metrics under dissimilar network parameters and configurations. The experimental outcome represents that proposed trust method accomplishes a significant decrease in false positives rate and a rise in the rate of detection of truly malicious nodes associated with traditional non fine-grained schemes.

It Yuxin Liu et. al. 2016 [6] recommendation created trust key model with a defence arrangement, which utilizes grouping procedure to dynamically sifter out attacks like ballot-stuffing, bad-mouthing, and collusion for mobile ad hoc networks. Connected to untruthful recommendations between convinced timebased on quantity of compatibility of information, interactions, and closeness amongst the nodes.It only detect bad mounting attack. It does not provide location and time based attacks. The recommending node is selected based on three influences checked its trustworthiness: quantity of communications with the appraised node, harmony of view with the appraising node for resolving the problematic of the insufficiency of closeness to the estimating node knowledge. Recommendations are collected over an epoch of time to guarantee the uniformity of recommendations on condition that by a recommending node concerning the assessed node. Clustering technique is implemented to dynamically clean out recommendations between convinced timeframe based on: a). Quantity of communications (using confidence key), b). Compatibility of data, information with the appraised node (through unconventionality test) and c). Similarity between the nodes. Dissimilar nodes are selected in the estimation process to test the performance of the cleaning procedure against numerous mobile neighbourhoods and topologies.

N. Leone et al. 2006 [7] technique recommend a novel procedure to recognize malicious node affected by hole black attack and construct dimension estimations that are resilient to numerous compromised sensors even when they conspire in the occurrence. The methodology tracked in this paper is based on dimensions investigation and its applicability depends on the supposition that the measurements are associated under unaffected environments, while negotiated measurements interrupt such connections. The drawbacks of the scheme is that the dimensions encompass duplicate information. This will not sense irregular fluctuations in the spatial patterns.

A. Cerpa et. al. 2005 [9] provides information about routing security. It also provides detection of blackhole attack.One constraint of the projected method is that it workings based on a postulation that malevolent nodes do not effort as a group, even though this may occur in a actual condition. This paper does not provide group attacks problem. Node number, trust value generated during network initialization and threshold values are used to calculate confidence key. Confidence key is equal to product of threshold value, node value and trust key. This confidence key value is used to validate the node.

D. Son et. al. 2005 [10] provides information about recommendation based trust model for MANET. It successfully provides details and differentiated the dishonest and honest recommendations. This algorithm will not work on blackhole and location and time based attacks. Initially all the required parameters, number of nodes, and threshold value for the network. The proposed algorithm will detect black hole based attacks in the network and informed to the network. If other nodes are authenticated nodes then select nodes for path creation. Otherwise backup nodes are used to select different authenticated nodes from list.

M. Steinder et. al. 2004 [11] provides Context-Aware Security and Trust framework (CAST) for sensor network, in which numerous contextual information, such as battery status, communication channel status, and weather condition, are composed and then used to decide whether the mischievousness is probable an outcome of malevolent activity or not. This paper will not detected selective and blackhole attacks which can provides many security problems. Initially all the required parameters, number of nodes, and threshold value for the network. The proposed algorithm will detect black hole based attacks in the network and informed to the network. The threshold key is agreed as 0.65. The trust value is calculated from timestamp provided by network. This trust value along with confidence key is used for node authentication.

In such protocols, the deficiency is that if the packet is routed via *n* routes simultaneously, the energy consumption will be *n* times that of a single path route, which will seriously affect the network lifetime; similar research can be seen in multi-path DSR the AOMDV. Share-based multi-path routing protocols. The SPREAD algorithm in Krishna Goranthala et. al [14] is a typical share-based multi-path routing protocol. The basic idea of the SPREAD algorithm is to transform a secret message into multiple shares, which is called a (T ,M) threshold secret sharing scheme. The M shares are delivered by multiple independent paths to the sink such that, even if a small number of shares are dropped, the secret message as a whole can still be recovered.

The advantage of this algorithm is that through multi-path routing, each path routes only one share, and the attacker must capture at least T shares to restore nodal information, which increases the attack difficulty. Thus, the privacy and security can be improved. In the above research, the multi-path routing algorithms are deterministic such that the set of route paths is predefined under the same network topology. This weakness opens the door for various attacks if the routing algorithm is obtained by the adversary.

DOI:10.17605/OSF.IO/GS9FK

Marti et al. [15] suggested one of the first key approaches. The author proposed a watchdog and path-rater method implemented on the DSR protocol to reduce the impression of malevolent nodes on the throughput of the system. Such method has the foremost inadequacy that each packet drop is measured as mischievousness by a node irrespective of the purpose for the packet drop. Additionally, such method cannot identify the mischievous nodes in the case of receiver packet collision, ambiguous packet collision, partial dropping limited transmission power, and collaborative attacks.

Shakshuki*et al.* [16] proposed the Enhanced Adaptive Acknowledgement (EAACK) set of rules to identify mischievousness nodes in MANETs background using RSA and DSA digital signatures. Their method can authenticate and validate the acknowledgement data packets, but at the overhead of extra resources; it also necessitates pre-distributed keys for digital signatures.

IV. CONCLUSION

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. The packet loss possible reasons may be node mobility, queue overflow and interference. . Maximum present trust-based security arrangements for MANETs consider packet loss as a sign of probable attacks by means of malicious nodes. Packet loss detection, reaction and report to the MANET is a significant factor of any widespread safety solution. Before isolating mischievous nodes from the route in trust-based safety arrangements, a FGA of packet is essential to avoid false positives.Short of FGA of packet investigation, the performance of primary safety systems may cut down, resultant in the penalty of not guilty nodes and discontinuation of portions of the system network, although real malicious nodes remain undetected. This paper reviews the different fine grained analysis methods with advantages and limitations. It also discuss methods of packet loss avoidance in mobile adhoc network.

REFERENCES

[1] T. Camp, J. Boleng, and V. Davies, “A survey of mobility models for AdHoc network research,” Wireless Commun. Mobile Comput. Special Issue Mobile Ad Hoc Netw. Res., Trends, Appl., vol. 2, no. 5, pp. 483–502, Aug. 2002.

[2] R. Korsnes, K. Ovsthus, F. Y. Li, L. Landmark, and O. Kure, “Link lifetime prediction for optimal routing in mobile ad hoc networks,” in Proc. MILCOM, Oct. 17–20, 2005, vol. 2, pp. 1245–1251.

[3] M. Karthik and P. Senthilbabu, “PESR protocol for predicting route lifetime in mobile ad hoc networks,” in Proc. ICON3C, 2012, pp. 22–27.

[4] A. Kumar, S. Jophin, M. S. Sheethal, and P. Philip, “Optimal route life time prediction of dynamic mobile nodes in manets,” in Proc. Adv. Intell. Syst. Comput., 2012, vol. 167, pp. 507–517.

[5] Elisa Bertino, Daniele Midi, Muhammad Saleen Khan, Majid Iqbal Khan, “Fine Grained Analysis of Packet Loss in MANET”, IEEE, 2017, pp. 7798-7807.

[6] Yuxin Liu, Mianxiong Dong, Kaoru Ota, and Anfeng Liu, Active Trust: Secure and Trustable Routing in Wireless Sensor Networks, IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 11, NO. 9, pp-2013-2018, SEPTEMBER 2016.

[7] N. Leone et al., “The DLV system for knowledge representation and reasoning,” ACM Trans. Comput. Logic, vol. 7, no. 3, pp. 499–562, Jul. 2006.

[8] N. Ramanathan et al., “Sympathy for the sensor network debugger,” in Proc. ACM SenSys, San Diego, CA, USA, 2005, pp. 255–267.

[9] A. Cerpa, J. L. Wong, L. Kuang, M. Potkonjak, and D. Estrin, “Statistical model of lossy links in wireless sensor networks,” in Proc. IEEE IPSN, 2005, pp. 81–88.

[10] D. Son, B. Krishnamachari, and J. Heidemann, “Experimental analysis of concurrent packet transmissions in low-power wireless networks,” in Proc. ACM SenSys, San Diego, CA, USA, 2005, pp. 237–250.

[11] M. Steinder and A. S. Sethi, “Probabilistic fault localization in communication systems using belief networks,” IEEE/ACM Trans. Netw., vol. 12, no. 5, pp. 809–822, Oct. 2004.

[12] T. He et al., “Energy-efficient surveillance system using wireless sensor networks,” in Proc. MobiSys, 2004, pp. 270–283.

[13] I. Stojmenovic and X. Lin, “Loop-free hybrid single-path flooding routing algorithms with guaranteed delivery for wireless networks,” IEEE Trans. Parallel Distrib. Syst., vol. 12, no. 10, pp. 1023–1032, Oct. 2001.

[14] Krishna Goranthala “Routing Protocols in mobile Ad-hoc network” Master Thesis in CS,10 credit Supervisor at CS-UmU: Thomas Nilsson UMEA UNIVERSITY, Dept of CS SE-901 87 UMEA ,Sweden.

[15] S. Marti, T. J. Giuli, K. Lai, and M. Baker, ``Mitigating routing misbehavior in mobile ad hoc networks," in Proc. 6th Annu. ACM Int. Conf. Mobile Comput. Netw., 2000, pp. 255_265.

[16] E. M. Shakshuki, N. Kang, and T. R. Sheltami, ``EAACK_A secure intrusion-detection system for MANETs," IEEE Trans. Ind. Electron., vol. 60, no. 3, pp. 1089_1098, Mar. 2013.