RESEARCH ARTICLE OPEN ACCESS

Enhancing Security in Manets Communication Issues and Mechanisms

[1]R.Sujatha , [2]Dr.P.Srivaramangai

[1] Ph. D.Research scholar Dept of Computer Science, Maruthu pandiyar college of Arts & Science College, Thanjavur

[2]Assisitant Professor of Computer Science, Maruthu pandiyar college of Arts & Science College, Thanjavur

--************************----------------------------------

ABSTRACT:

MANET is one of the promising area in research and development. A MANET is a self configuring infrastructure with less wireless network. Each node is having ability to form a network by finding the suitable node to communicate for transferring data through radio waves. A mobile communication demands cooperation between the nodes. The selfish behaviour of intermediate nodes during packet transmission will lead to the negative impact. Behaviour of a node plays an important role. This paper analysis different security issues, trust mechanisms and proposes a trust evaluation security solution

Keyword: *MANET, Adhoc , Mobile access.*

--************************-----------------------------------

INTRODUCTION:

In recent years Mobile AD-HOC Networks have been widely used and there has been enormous growth of mobile wireless networks. Since access to a variety of mobile applications and services on the Internet. Services such as Information sharing, routing and location issues have found their own get ways to activated in mobile environments. For these issues, a mobile ad hoc network (MANET) system model is implemented

which consists of a group of wireless mobile nodes that are able to communicate with each other in the absence of a fixed network communications or centralized administration. MANET is measured to signify infrastructure less networking, in which nodes are created dynamically and set up a network, found routing among them to build their own network when needed. MANETs applications are almost booming since they provide of a flexible method to set up communications in situations where geographical constraints demand a distributed system without fixed base stations. For example, emergency rescue services such as hurricane and earthquake disasters, need to exchange critical information on the battleground through networking. In MANETs, nodes rely on network cooperation scheme to work well. If the participating nodes cooperate then the data can be sent successfully within the expected time. But behind a MANET there is a cost intensive action. Since each a mobile node, Should detecting routes and forward packets. It demands extra local security, memory, network-bandwidth, and energy.

MOTIVATION OF SECURITY

A mobile Communication simply works if nodes participate and forward additional node’s packets. On the other hand each node has to consider its imperfect resources (most especially its energy & security). The cooperation on these networks is frequently contact-based. Mobile nodes be able to directly communicate with each other if a contact occur (that is, if they are inside communication range). Supporting this cooperation is a cost demanding activity for mobile nodes. Thus, in the actual world, nodes could contain a selfish behavior, being disinclined to forward packets for others. Selfishness means that some nodes reject to forward other nodes' packets to accumulate their own resources.

RESEARCH OBJECTIVES

A Watchdog system overhears wireless traffic and analysis it to choose whether neighbour nodes are behave in a selfish method. While the watchdogs detect a selfish node it is clear as a positive detection (or a negative detection, if it is detect as a non selfish node).If one node have formerly detected a selfish node it can broadcast this information to additional nodes when a contact occur. This way, nodes contain second hand information regarding the selfish nodes in the network. The objective of our approach is to reduce the detection time and to improve the accuracy by reducing the effect of equally false negatives and false positives used in Ex-or encryption algorithm for more security.

ISSUES AND CHALLENGES

Mobile Ad-hoc Networks (MANETs) believe that mobile nodes controlled cooperate in order to work correctly. This cooperation is a cost-intensive action and some nodes can decline to cooperate, most important to selfish node behaviour. Thus, the general network performance might be seriously precious. The utilize of watchdogs is a well-known technique to detect selfish nodes. Though, the detection process achieve by watchdogs can fail, generate false positives and false negatives that be capable of induce to wrong operations. Moreover, relying on neighbouring watchdogs without help can guide to poor performance while detecting selfish nodes, in appearance of precision and speed. In occurrence of selfish node in routing, Packet delivery ratio and, Data Security, Throughput will be reduced and End to End Delay will be increased.

RESULT AND REVIEWS PROCESS

In Mobile Ad-hoc Networks (MANETs) sent believed that mobile nodes should perform their task cooperate in order to work correctly. This cooperation is a cost-intensive action and some nodes can decline to cooperate, due to their too selfish node behaviour. Since, the general network performance is seriously precious. The utilize of watchdogs is a well-known technique to detect selfish nodes. Though, the detection process achieve by watchdogs can fail, It generated false positives and false negatives which is capable of inducing wrong operations. Moreover, relying on neighboring selfish node will lead to poor performance. So detecting selfish nodes before band will improve the performance by increasing, Packet delivery ratio and, Data Security throughput.

In Mobile Ad –hoc Network, the nodes should perform their task in a controlled and cooperative way in order to finish the work correctly. This is one of the security issue in MANET which can not addressed directly by existing security mechanism. Trust management is crucial here to avoid the malicious node and to make me communication smoothly. There are two types of attacks in MANET. The first one is external attack, which causes traffic congestion by providing fake

Routing service or knowing disturbing the nodes by preventing them to provide service. The second one is internal attack in which opponent used to gain access in the network by malicious imprison action or sometimes compromising me participating node to behave in a malicious way. This paper analyzes various trust management measures.

CONCLUSION:

The multi-hop communication in MANETs can be a reliable communication, presently as the hand-off nodes are collaborate for a time, the adaptable nodes in the MANET is not ready to manage with unusual nodes. Due to Mobility of node network topology can't be maintain. The proposed approach enforces the nodes to collaborate. In the credit base approach the selfish nodes are punishing for their malicious action the non-malicious node are satisfied for their support in network functionality. Intended for detection and prevention of the selfishness attack we include proposed the Ex-or Encryption algorithm. After implement the algorithm, PDR and Throughput, security will increases End to End delay will be decrease., . So, MANETs can be more efficient and secure in data communication**.**

REFERENCES

- [1] S. Abbas, M. Merabti, D. ewellyn-ones, and K. Kifayat, "Lightweight sybil attack detection in manets," IEEE Syst. J., vol. 7, no. 2, pp. 236–248, Jun. 2013.
- [2] S. Bansal and M. Baker, "Observation-based cooperation enforcement in ad hoc networks" arXiv:cs.NI/0307012, 2003.
- [3] S. Buchegger and J.-Y. Le Boudee, "Self-policing mobile ad hoc networks by reputation systems," IEEE Commun. Mag., vol. 43, no. 7, pp. 101–107, Jul. 2005.
- [4] L. Buttyan and J.-P. Hubaux, "Enforcing service availability in mobile ad-hoc WANs," in Proc. 1st Annu. Workshop Mobile Ad Hoc Netw. Comput., 2000, pp. 87–96.
- [5] L. Buttyan and J.-P. Hubaux, Stimulating cooperation in selforganizing mobile ad hoc networks," Mobile Netw. Appl., vol. 8, pp. 579–592, 2003.