An Analytical Approach To Abate Routing Aggressions In Manet

Sreekanth Danda, K. Ravi Chand
1 Final year M.Tech student, EVMCET
2. Professor, H.O.D Department of CSE, EVMCET
Jonnalagadda, Guntur (Dist.), A.P.

ABSTRACT

Mobile Ad Hoc Network (MANET) is distinguished from other networks mainly by its self configuring and optimizing nature. These types of networks are without fixed infrastructure and are more prone to aggressions that occur in the network. The existing methodologies namely SMP and STP results its inefficiency in detecting aggressor's intrusion during collisions and have high routing MANET. This was accomplished by the Reactive Routing protocol like DSR in MANET. An Extended Dempster Shafer theory was used to detect the aggressions and Cryptographic schemes like RSA, Certificate Distribution are used to isolate the attack from the network. In this paper we deal with different types of aggressions which occur in the network layer. The following paper is organized as follows. Section I deals with Introduction .Section II describes different of types of aggressions in MANET. Section III deals with intended work and different Contrivance to isolate the routing aggressions in MANET. Section IV deals with related work. Section V concludes the work and gives the future scope.

Index terms

MANET, RSA, IDRS, Dempster Shafer theory.

I. INTRODUCTION

Mobile ad hoc network has been a challenging research area for the last few years because of its rapidly changing nature of its topology; MANET is an independent system of mobile routers connected by connectionless links. The routers are free to move randomly and organize themselves capriciously. Thus, the network's connectionless topology may change rapidly and unforeseeably. Such a network may operate in a standalone fashion. Due to a deficiency of infrastructure support, each node acts as a router, expedite data packets for other nodes..

II Aggression in Manets

There are different types of aggressions in MANET which occurs in all the layers of the network. In Network layer the active and passive aggressions are more important. The active aggressions are discussed in this following paper

A. Sleep Deprivation Aggression

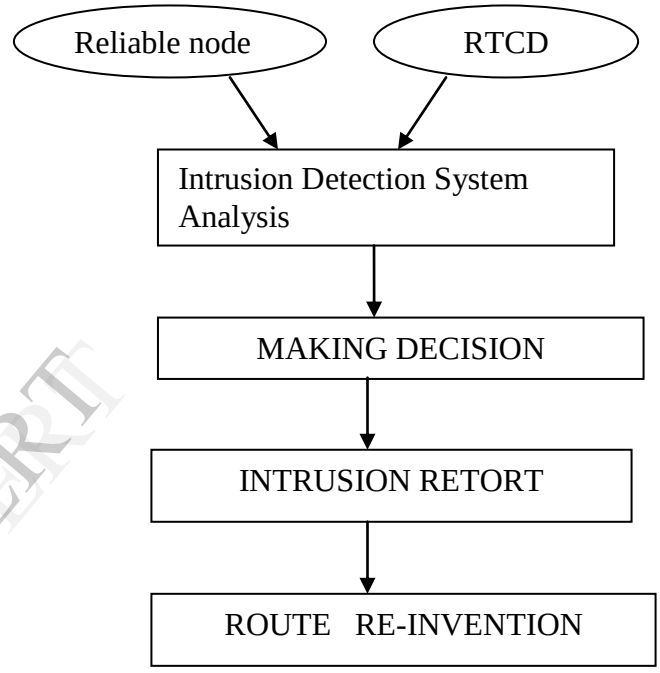
This kind of attack is actually more specific to the mobile ad hoc networks. The motto is to of restricted resources in the mobile ad hoc nodes (e.g. the battery powers), by unremittingly makes them busy processing unnecessary packets. In a routing protocol like DSR, sleep deprivation aggressions might be launched by flooding the targeted node with unnecessary routing packets. As a result, that particular node is unable to participate in the routing mechanisms and rendered unreachable by the other nodes in the network.

B. Link Spoofing Aggression

In link spoofing attack, an aggressor node advertises fake links with non-neighbours to disrupt routing operations. For example, in the DSR protocol, an aggressor can advertise a fake link with target's two-hop neighbours. This causes the target node to select the invalid path.

III.IDRS Analysis

The proposed work is to reduce the routing aggressions that take place in the network layer of MANET. So an Adaptive IDRS developed to perform the detection and avoidance of known routing aggressions and the proposed aggressions in the network layer. Here IDRS stands for Evidence Collection, Assessment of Risk, Decision making and Risk Response .In the Evidence. Collection phase the evidences are obtained from the reliable node and the routing table change detector. In the next step Assessment of risk is detected by using Extended Dempster Shafer theory .It is used for risk assessment calculation. Then based on these values the adaptive decision making process takes place .The Risk response is done by cryptographic schemes. This approach is implemented in the following way. Initially a reliable node is created and that node acts as (IDS/IRS).Further occurrence of an attack is confirmed and necessary measures are taken to detect, avoid and segregate the aggressions .Then the route is re-established by using this on demand. DSR is Reactive routing protocols which possess two phases namely Route Construction and Route Maintenance phases. It establishes the route only when it is needed by the source or destination node.



B. Resolution to Link Spoofing Aggression

The aggressor node is detected and avoided in the following way. Initially the aggressor node intentionally advertises the fake links to neighbour. The aggressor node is detected based on criterions like the Node which drop packets believing the fake links

.a) Evasion

Step1: Initially source node broadcasts key to every node to shortest path
Step2: The aggressor node which drops the packet is isolated from network by using Enhanced authentication protocol

EAP Contrivance involves these steps

1. Generation of nonce by both the server and client.

2. Generation of client ID, server ID takes place in both the server and client side
3. .Generation of master secret is done by using server ID in the server side
4. Generation of master secret is done by using client ID in the client side.
5. Then the master secret is transmitted to server side and then authenticated by server side.
6. Successful data transmission with success message.

D. Resolution to Sleep Deprivation Aggression.

The aggressor node is detected based on criterions Nodes which excessively flood packets to neighbour node, Battery power – zero.

a) Evasion

Step1: In earlier Energy levels of all nodes in the shortest path are determined by the reliable node (source node).
Step2: Then the packet routing takes place in that path. The aggressor node keep on flooding the packets and its energy level becomes zero(aggressor node is drained off)
Step 3: Once the packet has been reached the destination node, it replies with the acknowledgement. Meanwhile the aggressor node is drained off and its unable to reply to its neighbour. Within a TTL source node doesn't get the ACK packet.

IV Related Work

Some security related works has been proposed in MANET. An existing solution states that Reputation based security protocol is used in DSR to detect and remove malicious nodes. The key advantage of this protocol is that Black hole attack is detected easily and efficiently than AODV .Reference[1][2] gives an overview of the routing protocols such as ARAN, the known routing aggressions and the proposed countermeasures to these aggressions in various works In reference[4] new key management scheme is implemented in NTP protocol. Node Transition Probability (NTP) based algorithm provides maximum utilization of bandwidth during heavy traffic with less overhead.
NTP determines stable routes using received power. This proposal detects them modification, impersonation aggressions and TTL aggressions and avoids the effects of malicious node and provides appropriate measures to discard such malicious nodes in dynamic condition. Reference [3] proposed a new model called EIDAN makes use of Novel architecture to detect active aggressions. This model is very efficient in detecting resource consumption attack, fabrication attack. Reference[4] states that two trust models have been proposed namely probability model and entropy model. The malicious misbehaviour of nodes are characterized by these two models. The reliable value is assigned to be one .A trust graph is generated which is used to differentiate malicious nodes and good nodes. The proposed theoretical models are then applied to improve the performance of ad hoc routing schemes. Reference [5] proposed an extension to the TWOACK scheme, in which each node must send back a normal Ack to its immediate source node after receipt of any kind of packet.

V .Conclusion

We intended a risk-aware response resolution to abate for MANET routing aggressions. In this paper we developed an efficient IDRS analysis to detect and avoid the aggressions in the network layer .The Scope of future is to provide resolution to reduce various aggressions for routing packets in Manets

VI .References

[1] Soufiene Djahel, Farid Nait-abdesselam, and Zonghua Zhang fourth quarter 2011 "MitigatingPacket Dropping Problem in Mobile Ad HocNetworks: Proposals and Challenges" IEEECommunications surveys & tutorials, vol. 13, no. 4,

[2] Noman Mohammed, Hadi Otrok, Lingyu Wang,Mourad Debbabi, and Prabir Bhattacharya January-February 2011 "Mechanism Design-Based Secure Leader Election Modelfor Intrusion Detection in MANET" IEEE transactions on dependable andsecure computing, vol. 8, no. 1

[3] B. Kannhavong, H. Nakayama, Y. Nemoto, N.Kato, and A.Jamalipour, Oct. 2007 "A Survey of Routing Aggressions in Mobile Ad hoc Networks," IEEE Wireless Communication Magazine, vol. 14, no. 5.

[4] Kejun Liu, Jing Deng, Pramod K. Varshney, and Kashyap Balakrishnan, May 2007 "An Acknowledgment-Based Approach for the Detection of Routing Misbehavior in MANETs" IEEE transactions on mobile computing, vol. 6, no. 5.

[5] Amitabh Misgra and Ketan M. Nadkarni, ,2003, Security in Wireless Ad hoc Networks", in Book The Handbook of Ad hoc Wireless Networks(Chapter 30),CRC Press LLC.

AUTHOR-1 BIOGRAPHI

SREEKANTH DANDA M.Tech (CSE),
Final year student,
EVM COLLEGE OF ENGINEERING AND TECHNOLOGY,
,JONNALAGADDA,
GUNTUR (D.T)

AUTHOR-2 BIOGRAPHI

K. RAVICHAND. Professor,
H.O.D Department of CSE
EVM COLLEGE OF ENGINEERING AND TECHNOLOGY,
JONNALAGADDA,
GUNTUR (D.T)