International Journal of Advanced Research in

Computer Science Engineering and Information Technology

Volume: 2 Issue: 2 08-Mar-2014,ISSN_NO: 2321-3337

P_2P Intracommunity File Searching and Intrusion Detection in Manets

P.Selvi grija [1], J.Premkumar[2] , T.Sendhil kumar[3]
Assistant Professor, Department Of Computer Science and Engineering [#1]
PG Student, Department Of Computer Science and Engineering[#2,#3]
Chirst college of engineering and Technology, Puducherry, India.
Premkumar.pondy91@gmail.com[2]

ABSTRACT*-Mobile ad hoc network is one of most important research topics as they are infrastructure-less and mobile. Open medium, wide distribution and de-centralization of nodes makes MANETs vulnerable and malicious. It is crucial to develop efficient intrusion detection system to protect MANETs. A new intrusion detection system named bandwidth shared acknowledgment (BSA) in which all transmission packet data and acknowledge should be cryptographically signed. Swarm Based Detection techniques for multiple paths establishment among source to destination and random casting is use during intrusion in MANETs. Eavesdropping in MANET is scheduled based on number of acknowledgement received at every instance in network. The theme of this paper is to provide a seamless message delivery in a MANET despite its threats using random casting and the existing mechanisms like 2-hop acknowledgement or source directed acknowledgement does not hold when a network topology changes frequently or when a node is compromised. These drawbacks are to be addressed ensuring secured connecting edges between source and destination. The source collision, exposure to vulnerability is also minimized using this mechanism. We propose an optimize solution for above problem using BSA techniques which overcomes eaves dropping based on acknowledgement from intermediate only and P2P content-based file sharing system, namely Intracommunity File Searching, for disconnected MANETs. The system uses an interest extraction algorithm to derive a node's interests from its files for content-based file searching.*

Keywords *- Bandwidth Shared Acknowledgment (BSA), Mobile Ad Hoc Network (MANET), Random Casting, Swarm Detection.*

I, INTRODUCTION

Mobile Ad hoc Network (MANET) is a collection of mobile nodes equipped with both a wireless transmitter and a receiver that communicate with each other via bidirectional wireless links either directly or indirectly. Industrial remote access and control via wireless networks are becoming more and more popular these days. One of the major advantages of wireless networks is its ability to allow data communication between different parties and still maintain their mobility. However, this communication is limited to the range of transmitters. This means that two nodes cannot communicate with each other when the distance between the two nodes is beyond the communication range of their own. MANET solves this problem by allowing intermediate par-ties to relay data transmissions. This is achieved by dividing MANET into two types of networks, namely, single-hop and multihop. In a single-hop network, all nodes within the same radio range communicate directly with each other. On the other hand, in a multihop network, nodes rely on other intermediate nodes to transmit if the destination node is out of their radio range.

In contrary to the traditional wireless network, MANET has a decentralized network infrastructure. MANET does not require a fixed infrastructure; thus, all nodes are free to move randomly. MANET is

capable of creating a self-configuring and self-maintaining network without the help of a centralized infrastructure, which is often infeasible in critical mission applications like military conflict or emergency

Minimal configuration and quick deployment make MANET ready to be used in emergency circumstances where an infrastructure is unavailable or unfeasible to install in scenarios like natural or human induced disasters, military conflicts, and medical emergency situations.

Owing to these unique characteristics, MANET is becoming more and more widely implemented in the industry. However, considering the fact that MANET is popular among critical mission applications, network security is of vital importance. Unfortunately, the open medium and remote distribution of MANET make it vulnerable to various types of attacks.

For example, due to the nodes' lack of physical protection, malicious attackers can easily capture and compromise nodes to achieve attacks. In particular, considering the fact that most routing protocols in MANETs assume that every node in the network behaves cooperatively with other nodes and presumably not malicious, attackers can easily compromise MANETs by inserting malicious or non cooperative nodes into the network. Furthermore, because of MANET's distributed architecture and changing topology, a traditional centralized monitoring technique is no longer feasible in MANETs. in such case, it is crucial to develop an intrusion-detection system (IDS).

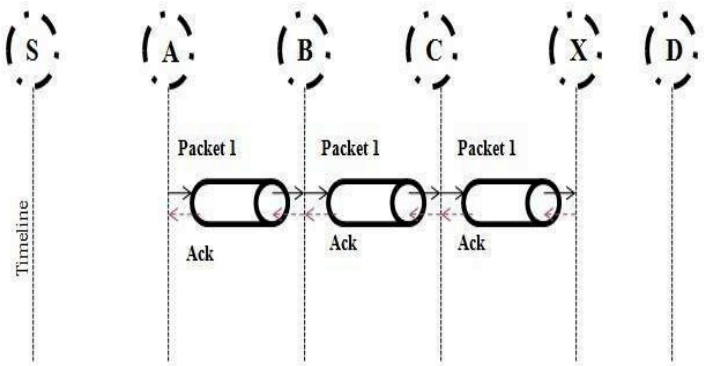
2,RELATED WORK

2.1IDS in MANETs

As discussed before, due to the limitations of most MANET routing protocols, nodes in MANETs assume that other nodes always cooperate with each other to relay data. This assumption leaves the attackers with the opportunities to achieve significant impact on the network with just one or two compromised nodes. To address this problem, an IDS should be added to enhance the security level of MANETs. If MANET can detect the attackers as soon as they enter the network, we will be able to completely eliminate the potential damages caused by compromised nodes at the first time. IDSs usually act as the second layer in MANETs, and they are a great complement to existing proactive approach.

2.2 Bidirectional Bandwidth Sharing

Bandwidth shared bi-directional MANETS for n-way acknowledgement for detecting an eavesdropping in MANET.



Shared Bandwidth N Way Acknowledgement

It initiate starts from source to destination then it check for multiple path bandwidth in an intermediate node if multipath then it compute the bandwidth for each multiple path if incoming bandwidth is greater than that sum of multiple path then it share incoming data based on frequency are else it fragment data from the previous input .check for least bandwidth and serve the minimum bandwidth and distribute same amount of data through bandwidth till minimum bandwidth. Do transfer at constant rate and constant delay.

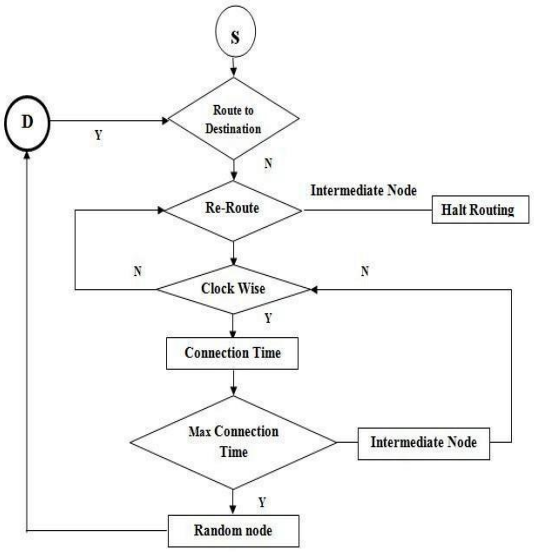
2.3 Swarm based detection

In this technique, the nodes with highest trust value, residual bandwidth and residual energy are selected as active nodes using swarm intelligence. Each active node monitors its neighbour nodes and estimates the delay is constant. It initiate data from intermediate node to destination and then calculate allocated bandwidth between the node calculate delay for one packet trough bandwidth.

2.4 Random Casting

A new communication mechanism is RandomCast, via which a sender can specify the desired level of overhearing, making a prudent balance between energy and routing performance. In addition, it reduces redundant rebroadcasts for a broadcast packet, and thus, saves more energy. Extensive simulation using ns-2 shows that RandomCast is highly energy-efficient compared to conventional 802.11 as well as 802.11 PSM-based schemes, in terms of total energy consumption, energy good put, and energy balance. In random casting, the server gets request from the client and gives response back through the IP address.

In mobile ad hoc networks (MANETs), every node overhears every data transmission occurring in its vicinity and thus, consumes energy unnecessarily. However, since some MANET routing protocols such as Dynamic Source Routing (DSR) collect route information via overhearing, they would suffer if they are used in combination with PSM. Allowing no overhearing may critically deteriorate the performance of the underlying routing protocol, while unconditional overhearing may offset the advantage of using PSM. Zheng and Kravets suggested a similar approach, called On-Demand Power Management (ODPM), in which a node switches between the AM and PS mode based on communication events and event-induced time-out values. For example, when a node receives an RREP packet, it is better to stay in AM for an extended period of time (RREP time-out) because it will most probably need to forward data



Random casting

2.5 Digital Signature

Digital signatures have always been an integral part of cryptography in history. Cryptography is the study of mathematical techniques related to aspects of information security such as confidentiality, data integrity, entity authentication, and data origin authentication. The development of cryptography technique has a long and fascinating history. The pursuit of secure communication has been conducted by human being since 4000 years ago in Egypt, according to Kahn's book in 1963. Such development dramatically accelerated since the World War II, which some believe is largely due to the globalization process.

The security in MANETs is defined as a combination of processes, procedures, and systems used to ensure confidentiality, authentication, integrity, availability, and nonrepudiation. Digital signature is a widely adopted approach to ensure the authentication, integrity, and nonrepudiation of MANETs. It can be generalized as a data string, which associates a message (in digital form) with some originating entity, or an electronic analog of a written signature.

Digital signature schemes can be mainly divided into the following two categories.

Digital signature with appendix: The original message is required in the signature verification algorithm. Examples include a digital signature algorithm (DSA).

Digital signature with message recovery: This type of scheme does not require any other information besides the signature itself in the verification process. Examples include RSA .

In this research work, we implemented both DSA and RSA in our proposed BSA scheme. The main purpose of this implementation is to compare their performances in MANETs.

The general flow of data communication with digital signature. First, a fixed length message digest is computed through a prepared hash function *H* for every message *m*. This process can be described as

$$H(m) = d. \qquad (1)$$

Second, the sender Alice needs to apply its own private key $P_{r\text{-}Alice}$ on the computed message digest *d*. The result is a signature Sig_{Alice}, which is attached to message *m* and Alice's secret private key

$$^{S}P_{r\text{-}Alice}(d) = Sig_{Alice} \qquad (2)$$

To ensure the validity of the digital signature, the sender Alice is obliged to always keep her private key $P_{r\text{-}Alice}$ as a secret without revealing to anyone else. Otherwise, if the attacker Eve gets this secret private key, she can intercept the message and easily forge malicious messages with Alice's signature and send them to Bob. As these malicious messages are digitally signed by Alice, Bob sees them as legit and authentic messages from Alice. Thus, Eve can readily achieve malicious attacks to Bob or even the entire network.

Next, Alice can send a message *m* along with the signature Sig_{Alice} to Bob via an unsecured channel. Bob then computes the received message m^{-} against the preagreed hash function *H* to get the message digest *d*. This process can be generalized as

$$H(m) = d \qquad (3)$$

Bob can verify the signature by applying Alice's public key P_{kAlice} on Sig_{Alice}, by using

$$^{S}P_{k\text{-}Alice}(Sig_{Alice}) = d. \qquad (4)$$

If $d == d$, then it is safe to claim that the message *m* transmitted through an unsecured channel is indeed sent from Alice and the message itself is intact.

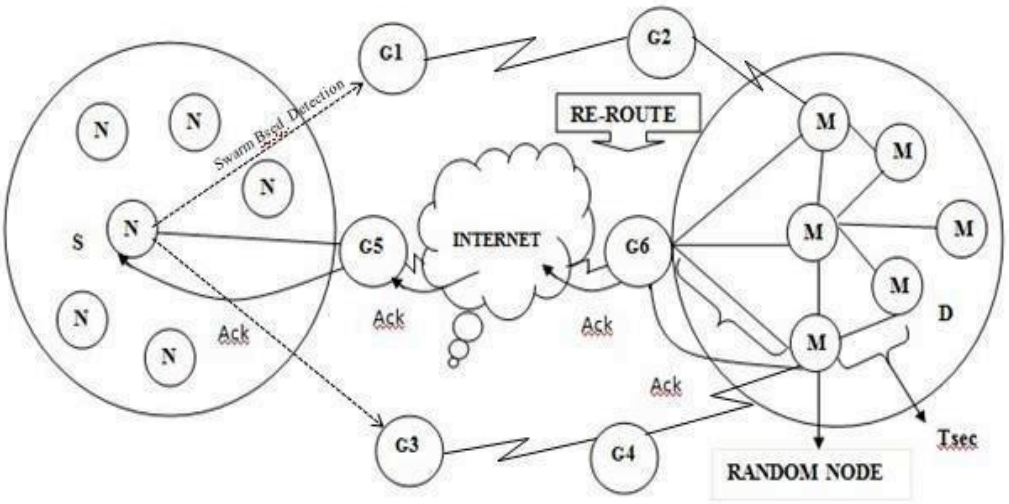
2.6 P2P File Sharing in Disconnected MANETs

The disconnected MANETs are featured by sparse node density and intermittent node connection, which makes previously introduced methods infeasible in such networks. We then further introduce two categories of P2P file sharing methods for disconnected MANETs.

3,SYSTEM MODEL

The overall system explain bi directional bandwidth acknowledgment (BSA) for intrusion detection (all transmission packet data and acknowledge should be cryptographically signed) random casting algorithm is used for multiple path selection making a prudent balance between energy. In addition, it reduces redundant rebroadcasts for a broadcast packet, and thus, saves more energy. And swarm based detection techniques for multiple paths establishment among source to destination to detect malicious based on nodes with highest trust value, residual bandwidth and residual energy are selected as active nodes using swarm intelligence based optimization. Each active node monitors its neighbour nodes and estimates the trust value.

P_2P file searching



Overall Design Architecture

It initiate starts from source to destination then it check for multiple path bandwidth in an intermediate node if multipath then it compute the bandwidth for each multiple path if incoming bandwidth is greater than that sum of multiple path then it share incoming data based on frequency are else it fragment data from the previous input .check for least bandwidth and serve the minimum bandwidth and distribute same amount of data through bandwidth till minimum bandwidth. Do transfer at constant rate and constant delay. Swarm based detection technique and Intracommunity File Searching for efficient node searching algorithm, the nodes with highest trust value, residual bandwidth and residual energy are selected as active nodes. using swarm intelligence. Each active node monitors its neighbour nodes and estimates the delay is constant. It initiate data from intermediate node to destination and then calculate allocated bandwidth between the node calculate delay for one packet trough bandwidth.

3.1 Bandwidth shared acknowledgement (BSA) algorithm

Bandwidth shared bi-directional MANETS for n-way acknowledgement for detecting an eavesdropping in MANET.

Algorithm

Step 1: initiate from source to destination. bw=bandwidth, IN=intermediate node

Step 2: check for multipath in IN

if multipath

{

compute bandwidth of each multipath

if(incoming(bw) > sum(multipath(bw))

share the incoming data based on frequency

else

fragment data from the previous input }

Step 3: check for least bw in the multipath serve the minimum bandwidth distribute same amount of data through bandwidth till min bw

{

do data transfer at constant rate & constant delay

}

repeat step 3 until all bw are serviced

Step 4 : end.

3.2.Swarm based detection algorithm

swarm based detection technique, the nodes with highest trust value, residual bandwidth and residual energy are selected as active nodes using swarm intelligence. Each active node monitors its neighbour nodes and estimates the delay is constant. It initiate data from intermediate node to destination and then calculate allocated bandwidth between the node calculate delay for one packet trough bandwidth.

Algorithm

Step 1: initiate data from intermediate node to destination

Step 2: calculate allocated bw between the node calculate delay for1 packet through bw

Repeat step 1

Until all intermediate data is transferred to destination .

Step 3: compute entire delay for (n-1) packet

if (first delay ~ (n-1) packet delay)

Use the same path & split the data

else

reroute [by Random casting algorithm 3]

Step 4 : compute throughput, constant delay & the frequency

[through variable ,delay=constant, frequency=variable] bandwidth= constant & no drop/least drop

3.3. Random casting

RandomCast is a techniques in which a sender can specify the desired level of overhearing, making a prudent balance between energy and routing performance. In addition, it reduces redundant rebroadcasts for a broadcast packet.

Algorithm

step 1 : initiate source to destination connection Rn= random node

Step 2 : check if algorithm 1 or algorithm 2 misbehaves select a random node.

Step 3 : if(Rn !=source node , Rn = broadcast ,Rn!= rebroadcast , Rn= regenerate)

Step 4 : route through clock wise or anti clock wise

Step 5 : check for Rn to destination & check for connection time >+3 sec

Step 6 : repeat through step 3 to find another random node.

3.4. Intracommunity File Searching and Retrieval

searching. Algorithm 1 shows the pseudocode of the intracommunity searching algorithm.

Algorithm 1. Pseudocode of intracommunity file searching for query Q conducted by node N_i.

Procedure intraSearchForQ ()

if a neighbor nb of N_i matches query Q then N_i.sendQeuryTo(Q, nb)
else if Q.src = N_i then
if Sim($v_{Q,} v_c$)< T_s then

$Q.V_{dest=} V_{nc}$

N_i.sendThroughIRATo(Q,
N_C)
Else

N_i.rankNbByFitness()
overallF =0
for each neighbor nb of node N_i do overallF gets overallF F+(Q; nb)
N_i.sendQeuryTo(Q, nb)

if overallF > _ then break

else

if Q.hops < MaxHopthen
$Q.V_{dest=} V_Q$
N_i.rankNbByFitNess()

nb the neighbor with maximal fitness N_i.sendQeuryTo(Q, nb)

else
$Q.V_{dest=} V_{nc}$
N_i .sendThroughIRATo(Q, N_C)

4, CONCLUSION

Packet dropping attack has always been a major threat to the security in MANETS. The drawbacks in the existing techniques have been overcome by this new methodology, A secure techniques is swarm based detection for multiple paths establishment among source to destination to detect failure node in mobile ad hoc networks (MANET). Bidirectional bandwidth acknowledgment (BSA) for intrusion detection (all transmission packet data and acknowledge should be cryptographically signed) random casting for multiple path selection making a prudent balance between energy during an intrusion.

5, REFERENCES

[1] G.Indirani and K.Selvakumar, "Swarm based Intrusion Detection and Defense Technique for Malicious Attacks in Mobile Ad Hoc Networks",International Journal of Computer Applications (0975 – 8887),Volume 50– No.19, July 2012.

[2] I. D. Chakeres and E. M. Belding-Royer, "AODV Routing Protocol Implementation Design," in Proceedings of the International Workshop on Wireless Ad hoc Networking (WWAN), Tokyo, Japan, March 2004.

[3] J. Hortelano, J. Carlos and P. Manzoni "Watchdog Intrusion Detection Systems in MANETs" *IJCSNS* International Journal of Computer Science and *Network Security*,6(6):209_219, June 2006.

[4] K. Liu, J. Deng, P. K. Varshney, and K. Balakrishnan, "An acknowledgment-based approach for the detection of routing misbehaviour in MANETs," *IEEE Trans. Mobile Comput.*, vol. 6, no. 5, pp. 536–550, May 2007.

[5] L Massoulié and J Roberts" Bandwidth Sharing" IEEE/ACM *Trans on Networking*, Vol. 10, No. 3, June 2002.

[6] N. Kang, E. Shakshuki, and T. Sheltami, "Detecting misbehaving nodes in MANETs," in *Proc. 12th Int. Conf. iiWAS*, Paris, France, Nov. 8–10, 2010, pp. 216–222.