Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 4, April 2014, pg.701 – 706

RESEARCH ARTICLE

SECURE DATA TRANSMISSION IN MANETS USING DSR, AODV, TRUST PROTOCOLS

K.Sangeetha[1], K.Rajakumari[2]

[1] PG Student, IT Department & Anna University, India
[1] Assistant Professor, IT Department & Anna University, India
[1] sangeethakannancse@gmail.com; [2] raji1anju@gmail.com

Abstract—***MANETs may be an assortment of wireless mobile nodes forming a network while not victimization any existing infrastructure. Varied issues area unit principally thanks to the shortage of resources of those networks. The solutions for typical networks area unit sometimes not decent to supply economical adhoc operations. The wireless nature of communication and lack of security infrastructure raise many security issues. Increased accommodative Acknowledge (EAACK) one in all the Intrusion Detection System (IDS) mechanism that will increase the integrity IDS victimization digital signature, ACK digitally signed before its reach destination. In EACCK probabilities to create false acknowledgement. EACCK uses DSR routing protocol for characteristic the route. DSR causes additional Routing Overhead. Instead of DSR, AODV and TRUST protocols accustomed offer less end-to-end delay and routing overhead. Comparison of those protocol accustomed choose higher path to secure transmission between nodes.***

I. INTRODUCTION

Mobile Adhoc Network (MANET) could be a collection of mobile nodes equipped with both a wireless transmitter and a receiver that communicate with one another via bidirectional wireless links both directly or indirectly. one amongst the foremost advantages of wireless networks is its ability to permit digital communication between different users and still maintain their mobility. This communication is proscribed to the range of transmitters. The two nodes cannot communicate with one another when the space between the 2 nodes could be a far communication vary of their own. MANET solves this communication problem by allowing intermediate users to data transmissions. Allowing intermediate user is achieved by dividing MANET into two forms of networks, namely, single-hop and multi hop. All nodes within identical radio range communicate directly with one another is termed single-hop network. in a very multi hop network, nodes accept other intermediate users to transmit if the destination node is out of their radio range. In different to the normal wireless network, Edouard Manet includes a redistributed network infrastructure. In Edouard Manet all nodes ar liberated to move arbitrarily. Edouard Manet is capable of making a self-configuring and self-maintaining network while not the assistance of a centralized infrastructure. MANET is in style among serious mission applications; network security is of significant importance. The open medium and remote distribution of Edouard Manet create it susceptible to varied sorts of attacks. Example, by reason of the nodes lack of physical defend, malicious attackers will merely capture and compromise nodes to comprehend attacks. particularly, considering the very fact that the majority routing protocols in MANETs assume that each node within the network performs helpfully with alternative nodes and presumptively not malicious, attackers will merely compromise MANETs by inserting malicious or non-co-operative nodes into the network. Moreover, owing to Edouard Manet distributed design and moving topology, a conventional centralized observance technique is not any longer possible in MANETs.

ROUTING IN A MANETs

Routing in a very MANETs are as such totally different from ancient routing found on infrastructured networks. Routing in a very Manet depends on several factors as well as topology, choice of routers, initiation of request, and specific underlying characteristic that would function a heuristic to find the trail quickly and expeditiously. The low resource handiness in these networks demands economical utilization and therefore the motivation for best routing in unplanned networks. Also, the extremely dynamic nature of those networks imposes severe restrictions on routing protocols of routing management info among the nodes.

Proactive and Reactive Routing Protocols Adhoc routing protocols are often broadly speaking classified as being Proactive (or table-driven) or Reactive (on-demand). Proactive protocols mandates that nodes in a very Manet ought to keep track of routes to all or any doable destinations so once a packet must be forwarded, the route is already identified and might be like a shot used. On the opposite hand, reactive protocols use lazy approach whereby nodes solely discover routes to destinations on demand, a node doesn't want a route to a destination till that destination is to be the sink of knowledge packets sent by the node.

Proactive protocols have the advantage that a node experiences minimal delay whenever a route is required as a route is instantly hand-picked from the routing table. However, proactive protocols might not continuously be applicable as they ceaselessly use a considerable fraction of the network capability to take care of the routing data . To cope up with this defect, reactive protocols adopt the inverse approach by finding a route to a destination only if required. Reactive protocols usually consume a lot of less information measure than proactive protocols, however the delay to see a route is considerably high and that they can generally expertise an extended delay for locating a route to a destination before the particular communicate.

II. BACKGROUND

IDS in MANETs

Due to the restrictions of most Edouard Manet direction-finding protocols, nodes in MANETs assume that alternative nodes continually work at the side of one another to transmit information. This assumption leaves the attackers with the opportunities to realize vital impact on the network with only 1 or 2 compromised nodes. to talk this drawback, IDS ought to be additional to boost the safety level of MANETs. If Edouard Manet will establish the attackers as shortly as they enter the network, we are going to be able to utterly reject the potential harms caused by compromised nodes at the primary time. IDSs usually act because the second layer in MANETs, and that they ar an excellent balance to existing proactive approaches. During this section, we tend to primarily discuss 3 existing approaches, namely, Watchdog , TWOACK.

1.A) Watchdog: Marti et al. [6] projected a theme named Watchdog that goal to develop the outturn of network with the presence of malicious nodes. In fact, the Watchdog theme is contain of 2 parts particularly, Watchdog and Pathrater.

Watchdog is IDS for MANETs. it's to blame for distinctive malicious node misbehaviors within the network. Watchdog identifies malicious misbehaviors by promiscuously paying attention to its next hop's transmission. If a Watchdog node eavesdrops that its next node fails to forward the packet at intervals a definite amount of your time, it raises its failure counter. Whenever a node's failure counter beats a predefined threshold, the Watchdog node says it's misbehaving. during this case, the Pathrater work along with the routing protocols to avoid the reportable nodes in future transmission.
The Watchdog theme be unsuccessful to spot malicious wrongful conducts with the presence of the following: 1) restricted transmission power; 2) receiver collisions; 3) ambiguous collisions; 4) false misbehavior report; 5) collusion; and 6) partial dropping.
A. TWOACK: With relevancy the six weaknesses of the Watchdog theme, several researchers projected new strategies to unravel these issues. TWOACK projected by Liu et al. [5] is one amongst the foremost main methodologies among them. In TWOACK theme, every node is needed to remand Associate in Nursing acknowledgment packet to the node that's 2 hops left from it. The dissimilar to several alternative schemes, TWOACK is neither Associate in Nursing sweetening nor a Watchdog-based theme. Targeting to resolve the receiver collision and restricted transmission power issues of Watchdog, TWOACK identifies misbehaving links by acknowledging each knowledge packet transmitted over each 3 ordered nodes on the trail from the supply to the destination. Upon recovery of a packet, every node on the route is needed to remit associate acknowledgment packet to the node that's 2 hops far from it down the route. TWOACK is important to figure on routing protocols like Dynamic supply Routing (DSR) .The TWOACK theme with success solves the receiver collision and restricted transmission power issues in Watchdog. However, the acknowledgment method needed in each packet transmission method accessorial a big quantity of unwanted network overhead. thanks to the restricted battery power nature of Edouard Manet, such redundant transmission method will simply degrade the life amount of the complete network.

B. AACK: ACK is associate end-to-end acknowledgment theme is shown in Fig. 1. In Fig. 1, the supply node S sends out Packet1 with none overhead except a pair of b of flag representing the packet kind. All the intermediate nodes solely forward this packet. once the destination node D receives Packet1, it's necessary to remit associate ACK acknowledgment packet to the supply node S on the reverse order of an equivalent path. inside a predefined fundamental measure, if the supply node S obtains this ACK acknowledgment packet, then the packet transmission from node S to node D is no-hit.

C. EACCK: The EAACK theme was extended with the introduction of digital signature to forestall the assaulter from shaping acknowledgement packets. EAACK is consisted of 3 major elements, namely: Acknowledge (ACK), Secure-Acknowledge (S-ACK) and misdeed Report Authentication (MRA). so as totally differentiate|to tell apart} different packet sorts in numerous schemes, they enclosed a two-bit packet header in EAACK. in keeping with the web draft of DSR , there area unit six bits reserved in DSR header. In EAACK, 2 of the six bits were accustomed flag totally different variety of packets. within the planned theme it had been assumed that the link between every node within the network is bi-directional. what is more, for every communication method, each the supply node and therefore the destination node don't seem to be malicious. Unless such that, all acknowledgement packets delineated during this analysis area unit needed to be digitally signed by its sender and verified by its receiver.

C. i .ACK ACK is essentially Associate in Nursing end-to-end acknowledgement theme. It acts as a region of the hybrid theme in EAACK, planning to scale back network overhead once no network misdeed is detected. In ACK mode, node S initial sends out Associate in Nursing ACK knowledge packet ad1 P to the destination node D. If all the intermediate nodes on the route between node S and node D area unit cooperative and node D with success receives ad1 P, node D is needed to remit Associate in Nursing ACK acknowledgement packet ak1 P on an equivalent route however in a very reverse order. at intervals a predefined fundamental quantity, if node S receives ak1 P, then the packet transmission from node S to node D is triple-crown. Otherwise, node S can switch to S-ACK mode by causing out Associate in Nursing S-ACK knowledge packet to observe the misbehaving nodes within the route.

C. ii. S-ACKS-ACK theme is Associate in Nursing improved version of TWOACK theme projected by Liu et al.The principle is to let every 3 consecutive nodes add a gaggle to notice misbehaving nodes. for every 3 consecutive nodes within the route, the third node is needed to send Associate in Nursing S-ACK acknowledgement packet to the primary node. The intention of introducing S-ACK mode is to notice misbehaving nodes within the presence of receiver collision or restricted transmission power. In S-ACK mode, the 3 consecutive nodes (i.e. F1, F2 and F3) add a gaggle to notice misbehaving nodes within the network. Node F1 initial sends out S-ACK information packet to node F2. Then node F2 forwards this packet to node F3. once node F3 receives, because it is that the third node during this three-node cluster, node F3 is needed to remand Associate in Nursing S-ACK acknowledgement packet to node F2. Node F2 forwards back to node F1. If node F1 doesn't receive this acknowledgement packet inside a predefined fundamental quantity, each nodes F2 and F3 ar reportable as malicious. Moreover, a misbehaviour report are going to be generated by node F1 and sent to the supply node S. one s adP one s adP one s akP one s akP. still, not like TWOACK theme,where a supply node straight off trusts the misconduct report, EAACK needs the supply node to modify to MRA mode and make sure this misconduct report.

C. iii MRA

The misconduct Report Authentication (MRA) theme is meant to resolve the weakness of Watchdog once it fails to observe misbehaving nodes with the presence of false misconduct report. False misconduct report will be generated by malicious attackers to incorrectly report that innocent nodes as malicious. This attack will be deadly to the whole network once the attackers break down decent nodes and therefore cause a network division. The core of MRA theme is to manifest whether or not the destination node has received the reported missing packet through a special route. To initiate MRA mode, the supply node initial searches its native data ase and seeks for different route to the destination node. If there's none different exists, the supply node starts a DSR routing request to seek out another route. because of the character of MANETs, it's common to seek out out multiple routes between 2 nodes. By adopting another route to the destination node, we have a tendency to circumvent the misconduct newsperson node. once the destination node receives AN MRA packet, it searches its native mental object and compare if the reported packet was received. If it's already received, then it's safe to conclude this is often a false misconduct report and whoever generated this report is marked as malicious. Otherwise, the misconduct report is trustworthy and accepted. By the adoption of MRA theme, EAACK is capable of sleuthing malicious nodes despite the existence of false misconduct report.

C. iv. DSA/RSA: EACCK has 3 components specifically, ACK,S-ACK,MRA square measure acknowledgement based mostly detection schemes. They all relay on acknowledgement packets to notice misbehaviours within the network. Thus it's very vital to confirm that everyone acknowledgement packets in EACCK square measure authentic and unsullied. otherwise, if the attackers square measure sensible enough to forge acknowledgement packets, all of the 3 schemes are vulnerable. With relevancy this imperative concern, in planned to company digital signature. In order to confirm the integrity of IDS,EACCK needs all acknowledgement packets to be digitally signed before they're sent out and verified till they're accepted.1024 bit DSA key and 1024 bit RSA key has been generated for each node within the network. Both a publickey and personal key distributed prior to. The typical size of public and personal key square measure 654b and 509b with 1024 DSA key and public key ,private key of 1024 RSA key square measure 272b and 916b.The signature size of RSA and DSA square measure 89B and 131B.DSAscheme continuously turn out less network overhead than RSA and also the signature size of DSA abundant smaller than the signature size of RSA. Routing Overhead (RO) differences between RSA and DSA schemes vary with totally different variety of malicious nodes. More variety of malicious nodes needs no acknowledgement packets, thus increasing the magnitude relation of digital signature within the whole network overhead. DSA needs additional battery power than RSA. Considering the trade-off between battery power and performance, DSA remains desirable.

III. PROBLEM DEFINITION

DSR performs multiple route discovery and no route repair strategies in DSR. So DSR has additional end-to-end delay, it will increase the output of the network DSR supported supply routing mechanism, if any link failure happens within the network ,DSR send a unicast packet to the supply giving the data concerning the broken link however supply might modification dynamically. DSR has additional routing overhead, less frequent route discovery and E2E delay. DSR will increase the network overhead.

IV. PROPOSED SYSTEM

Instead of DSR for distinctive the route, AODV and TRUST protocols area unit used. AODV is that the adhoc on demand distance vector provides less end-to-end delay than DSR by exploitation routing table. It calculates values of neighbor node nf realize path to supply secure transmission. It will rectify the broken link and its conjointly offer less routing overhead by providing high vary of packet delivery quantitative relation. A Hybrid Trust based mostly Routing Model used for identifying route .Every node finds its neighbor nodes and calculates the Trust price. The Trust price is calculated on 2 basis: Physical, Logical. Physical considers the Physical Network Parameters like information measure and Energy consumption. With the Variation within the information measure and therefore the energy used, our planned models analysis the trust quantitative relation for every node within the network. Logical Trust Model includes the 2 intrinsic parameters like Affinity and Trustworthy. Affinity is that the no.of dealings already created between the 2 nodes and its measures. Trustworthy measures the no.of booming and honest transactions between the nodes. With these measures, The trust price is calculated for every node. After Analyzing the trustworthy Nodes, The communication route are discovered. When associate un-trusted node tries to intrude the network, which will be intimated to the sender. Trust nodes provides higher finish to finish delay and output and fewer routing overhead than DSR and AODV. Because it uses trust nodes for distinctive the route. Trust provides the higher utilization of booming transmission through those nodes. So it provides higher output than different protocols.

V. PERFORMANCE EVALUATION

A. Simulation Configurations

Our simulation is conducted at intervals the Network machine (NS) a pair of.34 atmosphere on a platform with GCC four.3 and Ubuntu ten.24. In NS 2.34, the default configuration specifies twenty five nodes in an exceedingly flat house with a size of 670 × 670 m. the utmost hops allowed during this configuration setting area unit four. The moving speed of mobile node is restricted to twenty m/s and an intermission time of a thousand s. for every theme, we have a tendency to ran each network scenario thrice and calculated the common performance.

to live and compare the performances of our projected theme, we stock on to adopt the Packet delivery quantitative relation performance metrics [13].

1)Packet delivery quantitative relation (PDR): It defines the quantitative relation of the amount of packets received by the destination node to the amount of packets sent by the supply node. it's been calculated for DSR,AODV and TRUST model. TRUST provides high PDR worth than different protocols by mistreatment trust nodes. Because of less end-to-end delay, it has way more quantitative relation of causation and receiving packets than DSR and AODV .

2)Latency Evaluation: it's been calculated for TRUST model DSR and AODV.DSR protocol has a lot of end-to-end delay and routing overhead. if simulation time will increase, performance reflects as a lot of delay in transmission method. Due to less routing overhead in TRUST model by s mistreatment sure node it provides higher latency than DSR and AODV

3) output Evaluation: DSR performs multiple route discovery and no route repair strategies in DSR. So DSR has a lot of end-to-end delay, it will increase the output of the network. TRUST model has less routing overhead and end-to-end(E2E) delay

that has high output by mistreatment sure nodes. Number of causation and receiving packets will increase in owing to less E2E delay. TRUST model provides higher output than DSR.

VI. CONCLUSION AND FUTURE WORK

Time taken for sending via TRUST model is a smaller amount than the DSR and AODV.TRUST provides high PDR worth than alternative protocols by victimisation trust nodes. Because of less end-to-end delay, it has way more quantitative relation of causation and receiving packets than DSR and AODV. Due to less routing overhead in TRUST model by s victimisation trustworthy node it provides higher latency than DSR and AODV.TRUST model has less routing overhead and end-to-end(E2E) delay that has high outturn by victimisation trustworthy nodes. Number of causation and receiving packets will increase in as a result of less E2E delay. TRUST model provides higher outturn than DSR. In DSA, victimisation a similar worth double (even whereas keeping k secret),or employing a foreseeable worth, or unseaworthy even a number of bits of k in every of many signatures, is enough to interrupt DSA. Each RSA data formatting method needs the random choice of 2 terribly giant primes. In RSA over DSA, citing that RSA may be used for coding and digital signature applications, whereas DSA was strictly for digital signature application, the length of the plaintext which will be encrypted is proscribed to the scale of n. In fact, the $64000 length is even smaller than n thanks to the overhead introduced by the algorithms. As a result, the predominate approach is to get a random secret key and cypher that key with the RSA keys. The message is then encrypted employing a bilaterally symmetrical cipher with the generated secret key. With these limitations the EAACK approach must be any optimized for the digital signature schemes. In future, Instead of DSA/RSA Elliptic Curve Cryptography(ECC) is to supply a a lot of secured transmission. Eliptic curve cryptosystems area unit supported the separate index downside. Even if it uses shorter keysize, ECC provides same security level as RSA. The security of code is principally as a result of problem of resolution the elliptic curve separate index downside (ECDLP).So the attacks over code try and solve ECDLP downside. The main advantage of code is its high security level with smaller key size.

REFERENCES

[1] Elhadi M.Shakshuki, Nan Kang,Tarek R.Sheltami K.(2013)"EACCK-A Secure Intrusion Detection System for MANETs" IEEE Trans.Industrial Electronics,vol. 60,no. 3,pp. 1089-1098.

[2] Suneth Namal,Konstantinos Georgantas and Andrei Gurtov(2013) "Lightweight authentication and key management on 802.11 with eliptic curve cryptography",
IEEE Wireless communication and Networking conf., vol. 48, no. 5, pp 1830-1835.

[3] N.Kang,E.Shashuki and T.Sheltami,(2011)"Detecting forged

[4] Ackowledgements in MANETs"in proc IEEE Int.conf.AINA,Biopolis, vol. 15, no. 5, pp 484-497

[5] N.Naser and Y.Chen(2007) "Enhanced Intrusion Detection Systems for Discovering Malicious Nodes in Mobile Adhoc Network"in proc.IEEE int.conf.commun.,Glasgow,Scotland, vol .147 no.18 pp .384-387.

[6] K. Liu, J. Deng, P. K. Varshney, and K. Balakrishnan,(2007) "An Acknowledgment based approach for the detection of routing misbehaviour in MANETs," IEEE Trans. Mobile Comput., vol. 6, no. 5, pp. 536–55

[7] N. Kang, E. Shakshuki, and T. Sheltami,(2010) "Detecting misbehaving nodes in MANETs," in Proc. 12th Int. Conf. iiWAS, Paris,