COLLUDER DETECTION WITH SEAACK FOR INTRUSION DETECTION IN MANET

S.PRIYANKA[1]
PG Scholar
Kathir College of Engg
Coimbatore, TamilNadu, India
mailmepriya3091@gmail.com

V.ABINAYA[2]
PG Scholar
Kathir College of Engg
Coimbatore, TamilNadu, India
abinaya1391@gmail.com

S.S ARCHANA[3]
PG Scholar
RV S College of Engg. & Tech
Coimbatore, TamilNadu, India
ssarchanacse@gmail.com

Abstract— At present wireless networking has a global trend in the past few decades. The migration from wired environment to wireless environment has developed a lot due to its high mobility and scalability. The improved performances like high mobility and scalability made wireless environment more popular. Among all the contemporary wireless networks, MANET is referred as the one of the most important and unique applications. MANET does not require any fixed topology or fixed infrastructure. The main advantages of MANET are every single node can act as both transmitter and receiver, if not it will self configure to the neighboring nodes for successful transmission. The self configuring mechanism in MANET made it more popular wider and wider. MANETs are applicable even in the critical missions for example in military. Due to its advantages of MANET, it is introduced in industrial applications. The major drawback of using MANETs is its security issues as it does not require any fixed infrastructure. In this paper we propose a intrusion detection system named SEAACk specially designed to solve the security issues in MANET .And also we propose a new mechanism to avoid collusion by using the leak detector algorithm .Compare to all malicious detection mechanism SEAACk will provide higher detection without affecting the network performances

Keywords—*MANET,SEAACk,LEAK DETECTOR*

I. INTRODUCTION

Mobile Ad Hoc Network (MANET) is a collection of mobile nodes (hosts) which can communicate with each other through wireless links either directly or relying on other nodes as routers[6]. One of the major advantages of wireless networks is its ability to allow data communication between different parties and still maintain their mobility and scalability. MANET does not require any fixed infrastructure. Due to its natural mobility and scalability, MANETs are highly preferred for wireless networks since the first day of their invention. By definition, 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. Eventhough they have high mobility and scalability , this communication is limited to the range of transmitters which means that two nodes cannot communicate with each other when the distance between the two nodes is beyond the communication range of their own[7]. MANET solves this problem by allowing intermediate nodes to relay data transmissions. This can be achived by dividing MANET in to two types namely single-hop and multi-hop network. In single-hop all nodes within the same radio range communicate directly with each other hand. In a multihop network, nodes rely on other intermediate nodes to transmit if the destination node is out of their radio range. Owing to these unique characteristics, MANET is becoming more and more popular and it is implemented in the industry, However, considering the fact that MANET is popular among critical mission applications, network security is of consequential. MANETs open medium and remote distribution made it vulnerable to various types of attacks Furthermore, because of MANET's distributed architecture and changing topology, a centralized monitoring technique is no longer feasible in MANETs. In such case, it is difficult to develop an intrusion-detection system

(IDS). In the next section, we mainly concentrate on discussing the background information required for understanding this research topic

II. LITERATURE SURVEY

A. *Watch dog:* S. Marti, T. J. Giuli, K. Lai, and M. Baker proposed two schemes namely watchdog and pathrater[1] for identifying the misbehaving nodes in the network . Through simulation they have evaluated watchdog and pathrater using packet throughput, percentage of overhead (routing) transmissions, and this can fint the of misbehaving nodes in the network . when it reaches extreme mobility, watchdog and pathrater can increase network throughput by 27%, while increasing the overhead transmissions from the standard routing protocol's 12% to 24% the Watchdog scheme fails to detect malicious misbehaviors with the presence of the following: 1) ambiguous collisions; 2) receiver collisions; 3) limited transmission power; 4) false misbehaviour report;5)collusion; and 6) partial dropping.

B. *TWOACK:* In this K. Liu, J. Deng, P. K. Varshney, and K.Balakrishnan, proposed a scheme to detect the misbehaving links by acknowledging [2] all the data packet transmitted over every three consecutive nodes along the path from the source to the destination. By retrieving the packet, each node along the route is required to send back an acknowledgment packet to the node that is two hops away from it down the route. It is required to work on routing protocols such as Dynamic Source Routing . This scheme solves the receiver collision and limited transmission power problems. . The main idea of the 2ACK scheme is to send two-hop acknowledgment packets in the network allows the routing path to transmit in opposite direction . To reduce l routing overhead, only a fraction of the received data packets are acknowledged in the 2ACK scheme

C. *AACK:* This is an acknowledgment-based network layer scheme proposed by T. Sheltami, A. Al-Roubaiey, E. Shakshuki, and A. Mahmoud, which can be considered as a combination of a scheme called TACK [3](identical to TWOACK) and an end-to-end acknowl-edgment scheme called ACKnowledge (ACK). Compared to TWOACK, AACK significantly reduced network overhead while still capable of maintaining or even surpassing the same network throughput. In fact, many of the existing IDSs in MANETs adopt an acknowledgment-based scheme, including TWOACK and AACK. The functions of such detection schemes all largely depend on the acknowledgment packets. Hence, it is crucial to guarantee that the acknowledgment packets are valid and authentic. The concept of adopting a hybrid scheme in AACK greatly reduces the network overhead, but both TWOACK and AACK still suffer from the problem that they fail to detect malicious nodes with the presence of false misbehavior report and forged acknowledgment packets

D. *Leak detector*: K´alm´an Graffi, Parag S. Mogre, Matthias Hollick, and Ralf Steinmetz proposed a mechanism named leak detector for Wireless multihop networks such as Mobile Ad hoc Networks or Wireless Mesh Networks are proposed to satisfy the upcoming needs. Various security challenges arise because these networks work on the principles of node cooperation. A Leak Detector, is a mechanism to detect colluding malicious nodes in wireless multihop networks. By combining with proactive secure multipath routing algorithms, Leak Detector enables the calculation of the packet-loss ratio for the individual nodes and monitors the interruptions made physically.

III. EXISTING SYSTEM

In this section, we describe our existing work named EAACK scheme in detail proposed byElhadi M. Shakshuki,Tarek R. Sheltami. EAACK consisted of three major parts, namely, ACK, secure ACK (S-ACK), and misbehaviour report authentication (MRA). To distinguish different packet types in different scenarios they have included a 2-b packet header in EAACK. This i s by the Internet draft of Dynamic Routing Protocol[11].in this scheme,they have assumed that the link between each node in the network is bidirectional. And also, for each communication process both the source node and the destination node are not so malicious. Unless specified, all acknowledgment packets described in this research are required to be digitally signed by its sender and verified by its receiver.

ACK

ACK is intially an end-to-end acknowledgment scheme. in EAACK It acts as a part of the hybrid scheme, aiming to reduce network overhead when no network misbehavior is detected.

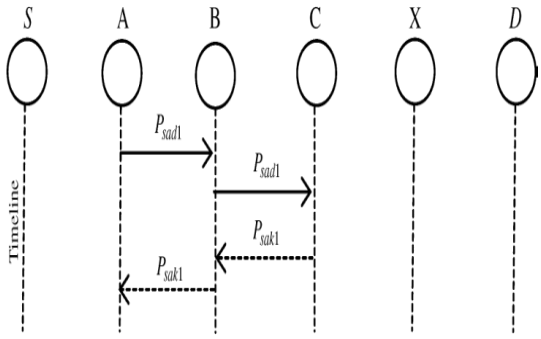

Fig 1: ACK scheme

When source node S in ACK mode, node S first sends out an ACK data packet P_{ad1} to the destination node D. If all the intermediate nodes in the network routes between nodes S and D are cooperative and node D successfully receives P_{ad1}, node D is required to send back an ACK acknowledgment packet P_{ak1} along the same route but in a reverse order. Within a predefined time period, if node S receives P_{ak1}, then the packet transmission from node S to node D is successful. Otherwise, node S will switch to S-ACK mode by sending out an S-ACK data packet to detect the misbehaving nodes in the route

S-ACK

The S-ACK scheme is an improved version of the TWOACK scheme proposed by Liu *et al.* . The principle is to let every three consecutive nodes work in a group to detect misbehaving nodes. For every three consecutive nodes in the route, the third node is required to send an S-ACK acknowledgment packet to the first node. The intention of introducing S-ACK mode is to detect misbehaving nodes in the presence of receiver collision or limited transmission power.EAACK requires the source node to switch to MRA mode in order to confirm the misbehaviour report. This is a consequential step to detect false misbehaviour report in the existing scheme.

MRA

The MRA scheme is designed to resolve the weakness of Watchdog when it fails to detect misbehaving nodes with the presence of false misbehaviour report. This report can be generated by malicious attackers to falsely report innocent nodes as malicious. To initiate MRA mode, the source node first searches its local base and seeks for an alternative route to the destination node. If there is no other that exists, the source node starts a DSR routing request to find another route. Due to the nature of MANETs, it is common to find out multiple routes between two nodes. By the adoption of MRA scheme, EAACK is capable of detecting malicious nodes with its existence of false misbehaviour report.

IV. PROPOSED WORK

SEAACk

A Secure Enhanced Adaptive Acknowledgement Scheme. It resolves the remaining two problems of watch dog such as Partial dropping and Ambiguous collisions by monitoring the Energy of all nodes which are in the network. Energy is the main problem in networks. The threshold value is fixed to each and every sensor. The sensor will be reconfigured when the energy touch its threshold value. the detailed explanation of the proposed work is explained by the help of block diagram shown below

CNDA

For detecting colluding misbehaving nodes without the use of cryptography, the mechanism named Leak Detector is used to detect colluding malicious nodes. It can be used in combination with any proactive, multipath, non-broadcasting, secure routing algorithm. The simulation work relates the contemporary IEEE 802.16 Mesh mode to measure the effects of colluding misbehaving nodes in WMNs. It can prominently able to tackle the problem of monitoring and presents good detection results, . The Leak Detector is one of the first mechanisms to address the problem of malicious colluding nodes in WMNs. To detect colluding misbehaviour and to identify malicious nodes. This information can be used to adapt routing strategies and to enable more dependable routing in MANETs.

Digital signature

Digital signature is a scheme which can be used for mathematical demonstration for verifying the authenticity of a digital message or a document. It is used as an integral part of cryptography till date. And also it i s used to ensure certain technique security such as entity authentication, confidentiality, data integrity, [7],data origin and authentication. Digital signature schemes can be mainly divided into the following two categorie

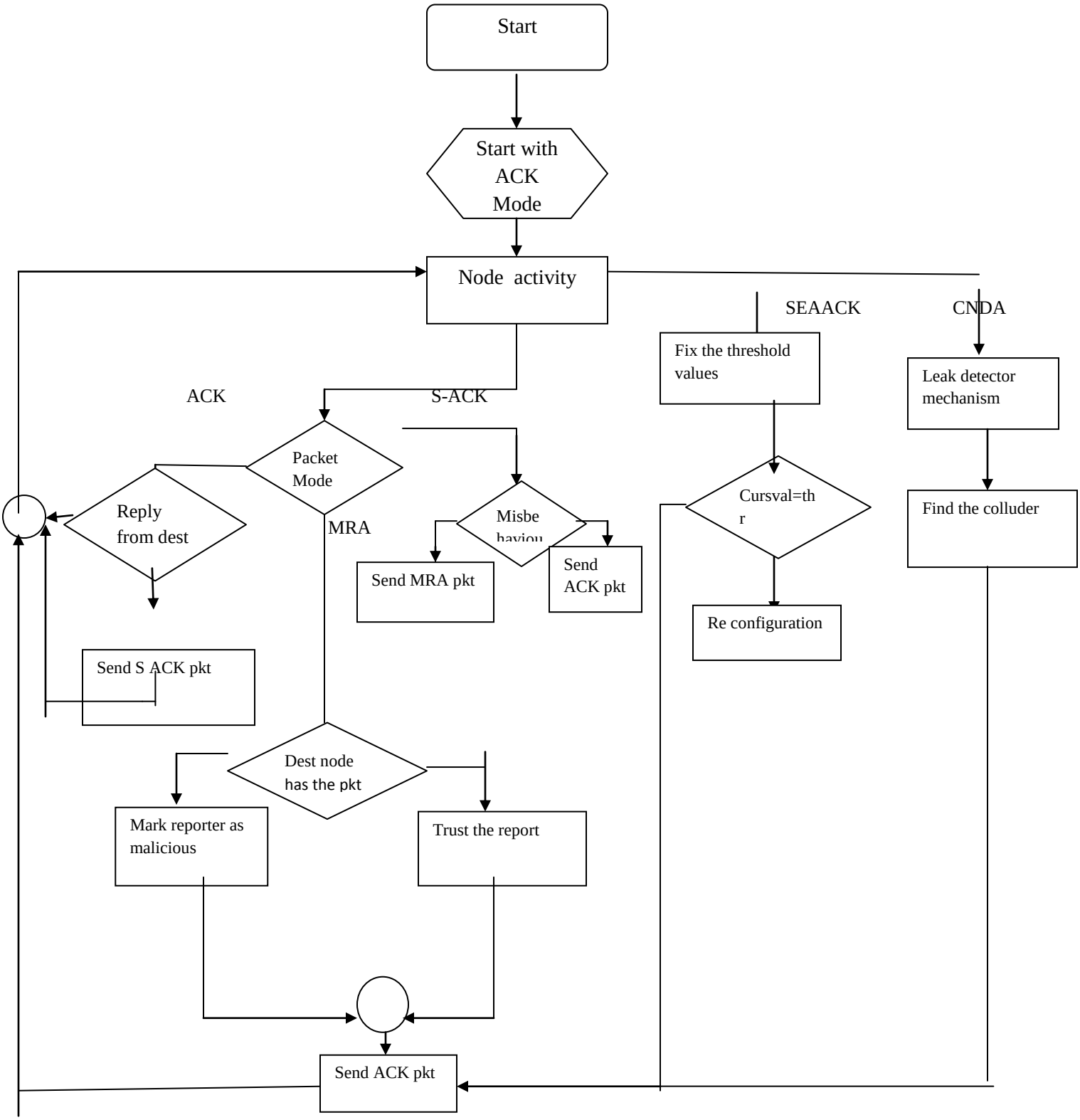

Fig2: SEAACK and CNDA scheme

V. CONCLUSION

Packet loss, ambiguous collision are the major drawbacks in the security issue of MANET. In this paper the propsed system introduces a new intrusion detection system(IDS) named SEAACK and CNDA for monitoring the colluder nodesThe proposed system also includes packet loss and automatic re-configuration if energy to reduce packets is lo collidropping and by using the st during transmission colluder detection algorithm monitors the network to find the attackers and remove that node from the networks

VI . REFERENCES

[1] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehaviour in mobile ad hoc networks," in *Proc. 6th Annu. Int. Conf. Mobile Comput. Netw., Boston, MA, 2000, pp. 255–265.*

[2] 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

[3] T. Sheltami, A. Al-Roubaiey, E. Shakshuki, and A. Mahmoud, "Video transmission enhancement in presence ofmisbehaving nodes inMANETs," *Int. J. Multimedia Syst., vol. 15, no. 5, pp. 273–282, Oct. 2009.*

[4] K´alm´an Graffi, Parag S. Mogre, Matthias Hollick, and Ralf Steinmetz *"Detection of Colluding Misbehaving Nodes in Mobile Ad hoc and Wireless Mesh Networks"*

[5] K. Kuladinith, A. S. Timm-Giel, and C. Görg, "Mobile *ad-hoc* commu-nications in AEC industry," *J. Inf. Technol. Const.*, vol. 9, pp. 313–323, 2004.

[6] Y. Kim, "Remote sensing and control of an irrigation system using a distributed wireless sensor network," *IEEE Trans. Instrum. Meas.*, vol. 57, no. 7, pp. 1379–1387, Jul. 2008.

[7] R. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Commun. ACM*, vol. 21, no. 2, 120–126, Feb. 1983

AUTOBIOGRAPHY

Ms.S.Priyanka has received her B.Tech degree in Information Technology from Anna university, Chennai and pursuing her M.E degree in Computer Science and Engineering under Anna University, Chennai. She has published 9 papers in National conferences. She has published 2 papers in international conference. she has attented 5 workshops related to her research work

Ms.V. Abinaya has received has received B.E degree in Computer Science and Engineering from Anna University,, Chennai and pursuing her M.E degree in Computer Science and Engineering under Anna University, Chennai. She has published 3 papers in National conferences. She has published 1 papers in international conference. she has attented too many workshops related to latest technologies.

Ms. ARCHANA.S.S has received B.E degree in Computer Science and Engineering from Anna University, Chennai with distinction and pursuing her M.E degree in Computer Science and Engineering under Anna University, Chennai. She has published 2 papers in National conferences. She has published 2 papers in international journal. She underwent in plant training for 5 days in some organizations to endure in her field