A Comprehensive Survey on Secure Intrusion Detection Systems for MANETs

Vishal U. Raut
M. Tech Student,
CSE Department, SGGSIE&T,
Nanded-431606, India.

M. S. Mahindrakar
Assistant Professor,
CSE Department, SGGSIE&T,
Nanded-431606, India.

ABSTRACT
In recent years, MANET become the foremost encouraging area for innovative work of the wireless communication system. It has inherited many vulnerabilities of wireless network because of open medium and self-organizing capability of nodes in MANETs. The intrusion detection system continuously observing for doubtful actions inside a system and then take proper action against them. There are many techniques for intrusion detection in wired system, however applying them directly into wireless environment is not possible. In this paper, we will see various well known intrusion detection system for MANETs with their problems and solutions. In this survey, latest intrusion recognition system specially designed for MANETs known as Enhanced Adaptive Acknowledgement system (EAACK) is discussed. This new scheme solves all the problems of existing intrusion detection systems such as detecting the malicious activities and the presence of false misbehaviour report.

General Terms
Digital signature, Enhanced adaptive acknowledgement, Misbehavior report authentication, Secure acknowledgement, Adaptive acknowledgement**.**

Keywords
Active and passive attacks, Dynamic source routing, Intrusion detection systems, Mobile ad hoc network, Vulnerability, Security.

1. INTRODUCTION
The wireless ad hoc networks has become the foremost dynamic field of communication networks, as a result the recognition of mobile devices and wireless communication system enhanced across the recent decades. In recent years, mobile ad hoc network (MANET) become the foremost encouraging area for innovative work of the wireless communication system [14]. Mobile ad hoc network [1] is an accumulation of mobile nodes organized through a both remote sender and recipient that share with each other through bidirectional wireless connections. The nodes can directly communicate with one another when they are both in the same transmission scope. Otherwise, they depend upon their specific nearby neighbours to broadcast the messages. The major advantages of wireless network is its capacity to permit the information correspondence between distinctive gatherings. This correspondence is restricted to the scope of transmitters. MANET resolves these issues by permitting middle nodes to depend on information transmission. The mobile ad hoc network can be used in different real time applications [6] such as military equipment, disaster recovery systems, and personal area networks.

The mobile ad hoc network has two forms of network as a single-hop and multi-hop [1]. A single-hop network includes many nodes among similar wireless range directly interconnect with one another whereas a multi-hop network includes nodes depend on alternative middle nodes to communicate when the getaway node is out of their own wireless range.

1.1 Vulnerabilities in MANET
MANETs are more susceptible in comparison with wired networks. In MANETs, a number of vulnerabilities [1]-[13] are represented below.

1.1.1 Absence of centralized administration
The lack of administration causes the recognition of assaults to be problematic, that it may not be easy to control the traffic in a highly energetic and expansive range of ad hoc network. This absence of unified administration may deal with operation of nodes.

1.1.2 Scalability
In a Scalability, size of ad hoc network changing constantly because of mobility of nodes. Consequently this is a main problem concerning security. Security systems ought to be fit for dealing with a huge system and little once.

1.1.3 Cooperativeness
Generally routing protocols [3] for MANET accepts that nodes become agreeable and non-malevolent. Subsequently a malevolent attacker can simply being a significant routing advisor as well as interrupt the network activity by resisting the protocol standards.

1.1.4 Restricted power source
In MANETs, the nodes are consider to be limited energy resource that result in few issues. In MANETs, a node is act like acquisitive way as soon as it is discovering that there is limited energy source.

1.2 Security Goals
Security involves a set of assumptions that are sufficiently subsidized. Within mobile ad hoc network, each of the networking capabilities like routing as well as package sending tend to be implemented through nodes in their own self-organized way. Hence, protecting a mobile ad hoc network must be highly demanding. Some security objectives [1] that secure the MANETs are defined below.

1.2.1 Availability
It means the resources become easily available to authorized individuals at particular instance. It can be applicable for each

data as well as services which guarantees the network services rather than Dos attack.

1.2.2 Confidentiality

It guarantees that computer system relevant resources can be utilized solely with recommended individuals. It needs to maintain the privacy of some secret data by keeping them secret from all objects that do not have rights to get them.

1.2.3 Integrity

It means that resources can be improved specially by approved parties in authorized way. This alteration contains composing, deleting, creating and changing status which assures that an information transmitted may be rarely damaged.

1.2.4 Authentication

It allows a node to confirm the recognition concerning with associate node that is interconnecting with this, which guarantees that participants in communication are authenticated.

1.2.5 Authorization

This one selects various access permissions in distinctive forms of individuals. For instance, a network management are often completed by only network manager.

1.3 Attacks in MANETs

MANETs tend to be susceptible to various forms of attacks especially concerning with the routing attacks [11]. In this section, we will see some typical attacks found in MANET. Generally these attacks are classified with many types as an active attacks and passive attacks [10]. In active attacks, intruder may actively capture the information stream and modifies its contents. The passive attack don't modify the contents of data stream but silently listen to it. The passive attack is launched to identify network vulnerabilities and to steal valuable information.

1.3.1 Wormhole attack

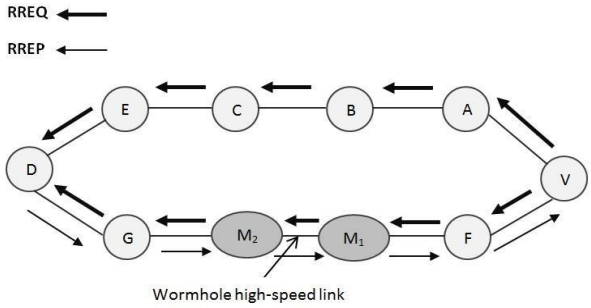

Fig 1: Wormhole attack [10]

It is one of the simple sophisticated attack [10] launched against routing in MANET. In this attack, two attacker creates a high speed link between them by means of either Ethernet cable or optical link. This connection termed as a wormhole link. These two conspiring nodes create deception that two remote regions are connected and these two nodes appear as neighbours of one another to rest of the network. They records data packet at one area and passage them through wormhole link to another attacker then second attacker transmit them to destination. As a significance of attack, path created through these two malicious nodes because route request (RREQ) arrived by this path takes minimal time to reach destination than others. After the path establishment, malicious nodes can easily damage the data stream flowing through them.

1.3.2 Rushing attack

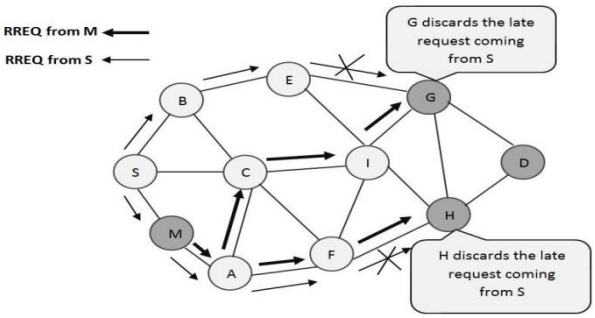

Fig 2: Rushing attack [10]

It is a forms of Dos attack [10] with all on demand routing protocols like DSR [15], AODV, etc. In on demand routing protocols, when any node wants for determining path up to the destination then he floods network with route request (RREQ). To limit the overhead of flooding, every node sends only one route reply (RREP) associated with that route discovery and drops all route request (RREQ) packet that arrives after first one. The attacker exploits this vulnerability of route discovery phase. For instance, consider a dynamic source routing [15] (DSR) as a routing protocol used for the path detection process. If route request (RREQ) forwarded by the attacker nodes are first one to reach neighbour of target then any succeeding authentic requests made are simply deleted by the neighbour of victim node. As a result of this attack, victim node is not able to find a path that doesn't include attacker node.

2. BACKGROUND

This section provides the information about background and previous things.

2.1 IDS in MANETs

Generally, the intrusion detection is a security innovation that makes an attempt to recognize entities who are attempting to interrupt into and abuse a framework without authorization and those who have appropriate access to the system have misuse their advantages [8]. The system secured is employed to specify a data system being checked by an intrusion detection scheme. The system can be a host or a network machines like a server, a firewall, a router or a corporate network, etc. An intrusion detection system may be an automatic data processing method which powerfully controls the technique and use activities within the network. In MANETs, intrusion detection systems are installed in every single node [2]. In this, mainly three existing intrusion detection systems are defined below.

2.1.1 Watchdog Scheme

This scheme [16] have two types mainly watchdog and pathrater. The watchdog works as an intrusion recognition for MANET which is responsible for identifying misbehaviour of malevolent nodes within the system [5]. It detects misbehaviour of malevolent node by randomly hearing to its following hop's distribution. In case of a watchdog node, it observes that subsequent node neglects for sending the packet in a predefined duration then nodes defeat counter increases. The watchdog node declares it as disobeying, whenever a nodes defeat counter increases a predetermined edge.

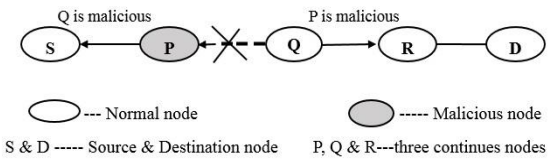

Fig 3: Watchdog scheme [16]

Fig. 3 demonstrates the operation of Watchdog system [16]. Whenever node P sends a packet coming from source node S in the direction of destination node D via node R, node P can't interconnect their distance in order to node R however it may accept within node Q's visitors. The node P could eavesdrop node Q's communication to confirm that node Q have tried to send the packet towards node R. The continues line specifies the projected path of packet supplied through node Q toward node R and dashed mark specifies node P is in the communication scope of Q which can eavesdrop packet transmission. The pathrater strategy permits the nodes to keep away from utilization of disobedient nodes in different forthcoming course choices. This transmitting data could approved with message. A Watchdog system can't be able to observe infectious misbehaviours in occurrence of ambiguous collision, receiver collision, restricted transmission power, incorrect misconduct report, collusion and partial dropping.

2.1.2 TWOACK Scheme

TWOACK system [11] proposed to detect a disobedient interfaces by recognizing each information packet transferred over each three continues nodes on a trail from source to the destination. It is needed to figure on routing protocols [3] like dynamic source routing.

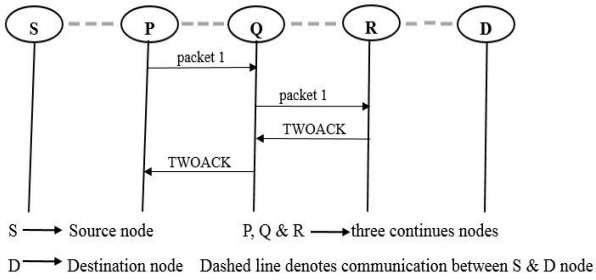

Fig 4: TWOACK scheme [11]

Fig. 4 demonstrates the working operation of TWOACK system [11]. Assume P, Q and R are three sequential nodes along a course from source to destination. Firstly node P sends packet 1 to node Q after that it send towards node R. At that point once node R acknowledge packet 1 since it is away from node P in two steps. Then, node R could required to create a TWOACK packet usually consists of inverse path from node R to P furthermore transfers this return towards node P. At node P, the retrieving of this TWOACK packet shows relaying of packet 1 can be recognized through node P to node R. In addition, both nodes Q and R happen to be stated as malevolent when these TWOACK packet is not accepted within a predefined duration. This one methodology does apply to each three progressive nodes through remaining path.

2.1.3 AACK Scheme

Generally an AACK system [17] is acknowledgment based network layer system similar to a TWOACK system, which may be thought of as a mix of a system called as a TACK furthermore overall recognition process referred to as an Acknowledge (ACK) system. It considerably decreases the network overhead as compared to TWOACK, whereas still ready to maintaining or maybe surpassing an equivalent network throughput. Fig. 5 demonstrates the working component of AACK system [17] as beneath.

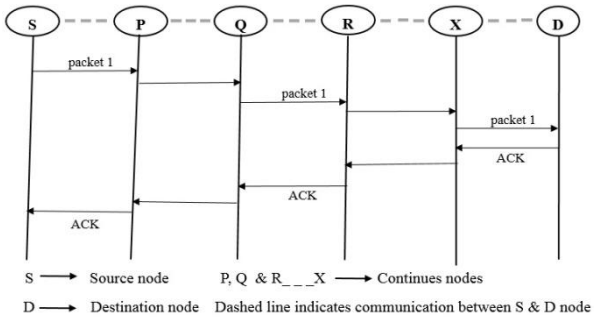

Fig 5: AACK scheme [17]

From figure 5, origin node S transmits packet 1 with no overhead with the exception about 2 b of flag. Each mediate nodes merely sends these packet. Once target node D accepts packet 1, it is obliged for transmitting again an ACK packet towards the source node S over the opposite direction of exactly same path. On the off chance that these source node S accepts ACK packet in a predefined time period, after that packet sending through node S to D is successful. Else, origin node S forwards a TACK packet by shifting on TACK system. By implementing the approach of hybrid system, enormously it diminishes system overhead, nevertheless TWOACK and AACK are affected by issue, because they are not able to recognize malevolent nodes in case of occurrence of incorrect misconduct report and false acknowledgment packets.

2.2 Drawbacks of existing IDSs in MANET

These exiting intrusion detection systems are suffered with different disadvantages. Watchdog has different drawbacks [16] that not able to identify disobeying nodes in occurrence of ambiguous collision, receiver collision, restricted transmission power, false misbehaviour report.

2.2.1 Ambiguous collision

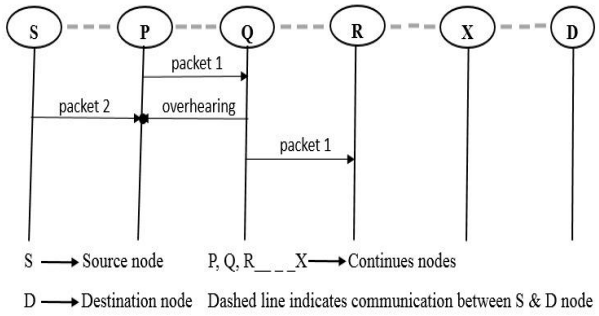

Fig 6: Ambiguous collision [16]

Fig. 6 shows the ambiguous collision [16], in which a dashed line indicates continues route from source to destination. Suppose three continues nodes P, Q and R are in a route from origin toward destination. From fig. 6,

- Firstly node P listens for node Q that will forward a packet 1 towards node R.
- Each packets 1 and 2 from node Q and S strike at node P is the ambiguous collision.
- In this instance, node P can't tell whether node Q is misbehaving or not.
- Keep concentrating on node Q for identify whenever it is misbehaving.

2.2.2 Receiver collision

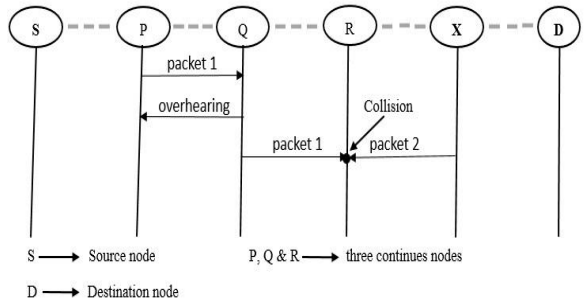

Fig 7: Receiver collision [16]

Fig. 7 shows the operation of receiver collision [16]. Firstly node P forwards packet 1 towards node Q. This packet attempts for discovering whether node Q transmitted such packet 1 towards node R, at the same time node X is transmitting packet 2 towards node R. In these types of circumstances, node P identify that node Q has securely transmitted packet 1 towards node R, nevertheless it may not be able to identify this node R. Because of accident in between packet 1 as well as packet 2 on node R, node Q was unable to accept packet 1. This would be a malicious action.

2.2.3 Restricted transmission power

Fig. 8 shows the operation of restricted transmission power [16]. Here node Q deliberately controls their communication strength in order to save individual power sources. Therefore, essentially this one is sufficient which overheard simply by node P however not sufficient to be obtained with node R.

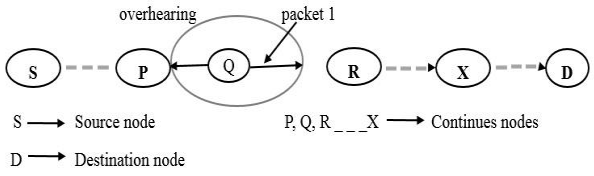

Fig 8: Restricted transmission power [16]

2.2.4 False misbehaviour report

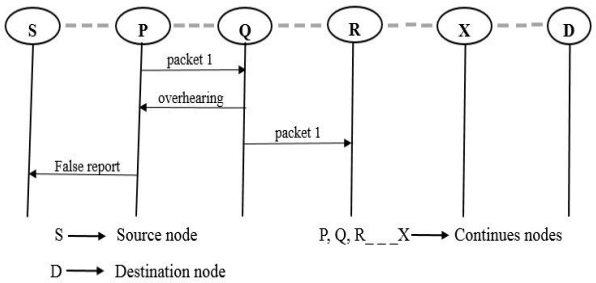

Fig 9: False misbehaviour report [16]

Figure 9 shows the operation of false misbehaviour report [16]. Even though node P effectively heard in which node Q sent packet 1 towards node R, nevertheless node P stated as node Q is mischievous. The invader may simply get along with agreement of one or two nodes, because of the active means as well as remote partition of distinctive MANETs for performing this false misbehaviour report attack.

- The TWOACK system effectively eliminates the receiver collision as well as restricted transmission power problems modeled by Watchdog. However, the acknowledgment procedure necessary in each packet transmission process included a significant amount of undesired network overhead. This undesired transmission procedure can easily reduce the life duration of the whole system because of limited battery power nature of MANETs.
- The concept of implementing a hybrid theme in AACK significantly decreases the network overhead, however TWOACK and AACK systems still experience the bad effects of the issue which will unable to identify malevolent nodes with occurrence of incorrect mischief report and fake acknowledgment packets.

2.3 Digital Signature

In MANET, nearly all present intrusion detection systems implement an acknowledgment based system consisting of TWOACK and AACK. The operations of these recognition systems depend upon the acknowledgment packets. So, this one is essential that will assurance the acknowledgment packets could be legitimate as well as original. In order to deal with such case, we are represent a digital signature system named as an Enhanced Adaptive Acknowledgement (EAACK). The digital Signature has been a very important portion of cryptography in history. The study of cryptography related with mathematical systems associated to the features of data security including privacy, information reliability, verification and also information source authentication [7]. In Egypt before 4000 years back, these detection systems relating with safe transmission may be directed by one using Kahn's book [18] in 1963. Significantly this progress improved since the World warfare II, which certain think that is generally due to globalization or economical system. A digital signature might be inclusively implemented method for affirming authentication, reliability and also non repudiation [7] of MANETs. Digital signature system [7] is partitioned into two sorts which includes a Digital Signature Algorithm (DSA) and Rivest Shamir Adleman (RSA) algorithm.

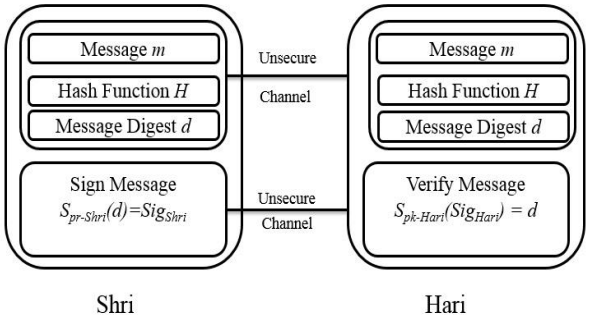

Fig 10: Communication with the digital signature [4]

Fig. 10 demonstrates the complete approach of information correspondence using digital signature [4]. Firstly, a limited size information process can be figured out with a predetermined hash attribute *H* for each information *m.* This procedure [4] may outlined as,

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

After that, a sender Shri requires its personal private key $P_{r\text{-}Shri}$ for applying on the computed processing information *d*. The conclusion will be a signature Sig_{Shri} that will connected to information *m* and Shri's secret private key.

$$S_{Pr\text{-}Shri}(d) = Sig_{Shri} \quad (2)$$

Frequently the sender Shri is required to remain her private key $P_{r\text{-}Shri}$ as a hidden without realizing to anybody other to confirm validity of the digital signature. Otherwise, he should acquires the information and simply copy malevolent information using Shri's signature, furthermore forward themselves towards Hari whenever attacker Om acquires such hidden private key. Since such malevolent information were digitally authorized with Shri, after that Hari considers them from Shri that information should be accurate and authentic. As a result, excitedly Om may accomplish malevolent attacks to Hari and also even the entire network.

Then, Shri could forward an information m using signature Sig_{Shri} towards Hari over an insecure channel. After that Hari computes accepted information *m'* instead of preagreed hash attribute *H* to obtain the information digest *d'*. Such procedure can be outlined as

$$H(m') = d. \quad (3)$$

By implementing Shri's public key $P_{k\text{-}Shri}$ on Sig_{Shri}, Hari should validate the signature, by utilizing

$$S_{Pk\text{-}shri}(Sig_{shri}) = d. \quad (4)$$

Once *d = = d',* consequently it is secure to declare that the information *m'* transferred using an insecure route which will be definitely transmitted from Shri and the information themselves is complete.

3. IDS proposed for MANET

In this section, we will see new different intrusion detection systems proposed for MANETs utilizing EAACK as demonstrated in fig. 11. It is proposed [12] to improve three faults of Watchdog system like false misbehaviour, restricted transmission power and receiver collision that can be already discussed. This technique also presented the idea of digital signature into intrusion detection system. It is an acknowledgement based intrusion detection system which needs less equipment cost. It also utilizes the digital signature system to stop attacker via replicating acknowledgment packets. Fig. 11. demonstrates overall architecture of the EAACK system.

The architecture of EAACK system is partitioned into following major parts as ACK scheme, S-ACK scheme, MRA scheme.

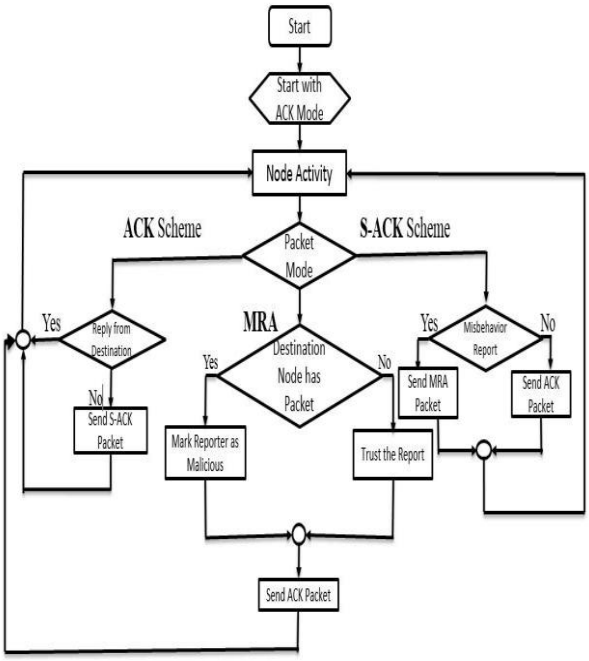

Fig 11: EAACK architecture [12]

3.1 ACK Scheme

An ACK is basically end-to-end acknowledgment scheme. It works as a part of the hybrid scheme in EAACK that aims to decrease the network overhead as soon as network misbehavior is not recognized. Fig. 12 shows the operation of ACK scheme.

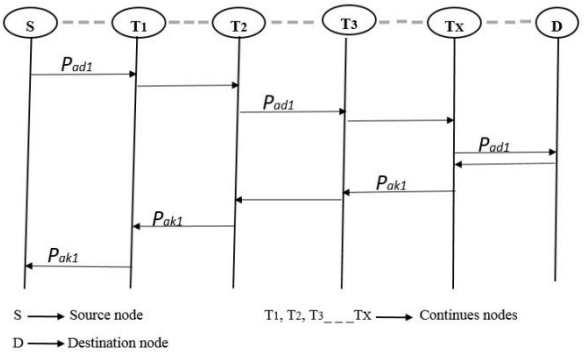

Fig 12: ACK schme [11]

In ACK system (T1, T2, T3, _ _ _Tx are continues nodes), firstly source node S forwards an ACK data packet Pad1 towards destination node D. When each middle nodes in direction from nodes S to D will be convenient furthermore node D successfully accepts packet Pad1, subsequently node D should be needed for forwarding back an ACK packet Pak1 in same path conversely in opposite request. Else, node S might shift on S-ACK manner by forwarding an S-ACK formation packet to detect the misbehaving nodes in the route.

3.2 S-ACK Scheme

The S-ACK system [11] is advanced type of the TWOACK system. The concept should allow each three continues nodes operates in a gathering for identifying mischief nodes. The important reason for introducing a S-ACK mode needs to

distinguish mischief nodes in the occurrence of receiver collision and restricted transmission power. Fig. 13 demonstrates the operation of Secure ACK scheme.

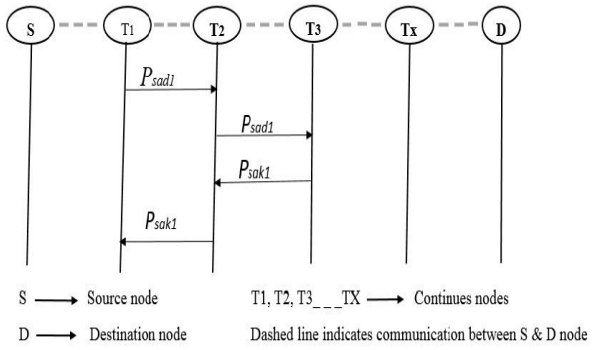

Fig 13: S-ACK schme [11]

In regards to S-ACK method, three successive nodes (i.e., T1, T2, and T3) works in gathering to identify mischief nodes within the system. Firstly node T1 forwards S-ACK information packet Psad1 towards node T2. When this occurs, node T2 forwards a packet towards node T3. Once node T3 gets packet Psad1 since it's a third node within this three node group, so node T3 is necessary in order to deliver back an S-ACK acknowledgment packet Psak1 towards node T2. At that instant, node T2 sends the packet Psak1 returning towards node T1. When node T1 will not get the acknowledgment packet in particular duration, after that nodes T2 along with T3 will be stated like malevolent. However, the misbehaviour report should be produced by node T1 furthermore this may be transferred towards a source node S.

3.3 Misbehavior Report Authentication Scheme

In S-ACK scheme, origin node instantly believes a misbehaviour report, so EAACK needs origin node to change into misbehavior report authentication system and verify such misbehaviour report. It can be a crucial phase to identify wrong misbehaviour report in recommended system. Whenever this one neglects for recognizing mischievous nodes in the occurrence of wrong misbehaviour report, then MRA system should intended to determine drawbacks associated with a Watchdog system. This kind of attack may be harmful for the complete system, once the attackers split out adequate nodes as well as reasons a system partition. The basis of MRA system should be affirmed even if the destination node has gotten the specified missing packet via various ways. Firstly origin node discovers their regional information base as well as another path to destination node to activate the MRA mode. When there is no different way, so origin node chooses the dynamic source routing requirement for discovering one other way. It is normal to figure out various paths between two nodes because of the nature of MANETs.

We avoid the misbehaviour reporter node by implementing another path to the destination node. Once the destination node receives a MRA packet, it discovers its regional information base as well as analyses when a reported packet has been recognized. When these packet has been previously recognized, subsequently this can be secure which determine that it can be a wrong misbehaviour report furthermore anyone who produced such report will be proclaimed to be malevolent. Else, this misbehavior report will be trusted as well as acknowledged. In such way, EAACK will become proficient for recognizing malevolent nodes instead of the occurrence of wrong misbehaviour report by implementing the MRA scheme.

3.4 Digital Signature

EAACK system has an acknowledgment dependent intrusion recognition system which includes ACK, S-ACK, and MRA schemes. These schemes based on acknowledgment packets for recognizing misbehaviours within the system. So throughout the EAACK system, this one will be very essential for confirming when every acknowledgment packets would be real as well as uncorrupted.

When the assailants will be sufficiently keen for copying acknowledgment packets, then the majority of three recognition systems are susceptible. Therefore, for overwhelming such issues digital signature is implemented in secure intrusion detection system. Usually EAACK system needs every ACK packets which will digitally authorized prior to those will be transmitted away as well as confirmed, till they would be acknowledged to confirm the integrity of intrusion detection system [9]. In this way, to deal with this concern we may utilize the digital signature schemes to discover most ideal solution for the security purpose of MANETs.

4. ACKNOWLEGMENTS

The authors are highly indebted to the authors of various research papers that are helpful for preparing this survey paper. The authors are also grateful to SGGSIE&T, Nanded for their support for completing this survey paper.

5. CONCLUSION

The actual MANETs usually are at the risk of different types of security attacks. Consequently, there is a main issue concerning their security. Here, we study several intrusion detection system approaches which provides more security to the MANETs. Nevertheless, many recent intrusion detection system have got some weakness and limitations such as a receiver impact, restricted transmission power as well as false misbehaviour report.

To address these issues, a new enhanced intrusion detection system i.e. EAACK scheme is proposed which usually solves the problems regarding recent intrusion detection systems. The actual major threats such as false misbehaviour report as well as forge acknowledgement packets can be discovered by utilizing this system. In MANETs, EAACK system greatly decreases complete delay of the system in comparison with the existing systems. As a result, it increases the throughput & efficiency of the system. This enhanced EAACK intrusion detection system makes the MANETs more secure and powerful. In future research, we will planning to eliminate the issues such as possibilities of implementing the hybrid cryptography methods to furthermore decrease the network overhead produced by digital signature and also checking the performance of EAACK in proper network environment.

6. REFERENCES

[1] Djenouri, Djamel, L. Khelladi, and N. Badache, "A survey of security issues in mobile ad hoc networks," IEEE communications surveys 7, no. 4, 2005, pp. 2-28.

[2] T. Anantvalee and J. Wu, "A Survey on Intrusion Detection in Mobile Ad Hoc Networks," in Wireless/Mobile Security. New York: Springer Verlag, 2008.

[3] W. Heinzelman, A. Chandrakasan, H. Balakrishnan, "An application-specific protocol architecture for wireless micro sensor networks," IEEE Transactions on Wireless Communications, 2002, pp. 660–670.

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

[5] J. Parker, J. Undercoffer, J. Pinkston, and A. Joshi, "On intrusion detection and response for mobile ad hoc networks," in Proc. IEEE Int. Conf. Perform., Comput. Communication, 2004, pp. 747–752.

[6] N. Nasser and Y. Chen, "Enhanced intrusion detection systems for discovering malicious nodes in mobile ad hoc network," in Proc. IEEE Int. Conf. Commun., Glasgow, Scotland, Jun. 24–28, 2007, pp. 1154–1159.

[7] A. Menezes, P. van Oorschot, and S. Vanstone, Handbook of Applied Cryptography. Boca Raton, FL: CRC, 1996, T-37.

[8] A. Patwardhan, J. Parker, A. Joshi, M. Iorga, and T. Karygi-annis, "Secure routing and intrusion detection in ad hoc networks," in Proc. 3rd Int. Conf. Pervasive Comput. Communication, 2005, pp. 191–199.

[9] Y. Zhang, W. Lee, and Y. Huang. (2003, Sep.). Intrusion Detection Techniques for Mobile Wireless Networks. ACM/Kluwer Wireless Networks Journal (ACM WINET), Vol. 9, No. 5.

[10] Wu, Bing, Mihaela Cardei, Jie Wu, Jianmin Chen, and Mihaela Cardei. "A survey of attacks and countermeasures in mobile ad hoc networks." In Wireless Network Security, pp. 103-135. Springer US, 2007.

[11] 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.

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

[13] R. Rishi, P. Goyal1, V. Parmar. MANET: Vulnerabilities, Challenges, Attacks, Application. IJCEM International Journal of Computational Engineering & Management, Vol. 11, January 2011.

[14] Q. M Alriyami, E. Asimakopoulou and N. Bessis. A Survey of Intrusion Detection Systems for Mobile Ad-Hoc Networks. IEEE International Conference on Intelligent Networking and Collaborative Systems, pp. 427-432. 2014.

[15] Johnson, D., Y. Hu, and D. Maltz. "The dynamic source routing protocol (DSR) for mobile ad hoc networks for IPv4." Vol. 260. RFC 4728, 2007.

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

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

[18] M. Zapata and N. Asokan, "Securing ad hoc routing protocols," in Proc. ACM Workshop Wireless Secur., 2002, pp. 1-10.