Indian Journal of Science and Technology, *Vol 10(16), DOI: 10.17485/ijst/2017/v10i16/112054, April 2017*
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

Prevention of Stealthy Attacks through Privacy Mechanism in Wireless Ad hoc Networks

D. V. Srihari Babu[1]* and P. Chandrasekhar Reddy[2]

[1]Department of Electronics and Communication Engineering, Kottam Karunakara Reddy Institute of Technology, Kurnool – 518218, Andhra Pradesh, India; Srihari2k1@gmail.com
[2]Department of Electronics and Communication Engineering, JNTUH College of Engineering, JNTUH Hyderabad – 500 085, Telangana, India

Abstract

Objectives: Stealthy attacks are a kind of attacks which injects route fabrication information and producing false identification in network. In this paper, we evaluate these two stealthy attacks against a privacy mechanism as Distinct Authentication Key Approach (DAKA) in MANET. **Methods/Statistical Analysis**: Wireless networks are becoming the most popular in today communication systems, where users prefer to have wireless connectivity regardless of its geographic location. However, the openness of wireless communications increases the threat to MANET under its conditions. It is very challenging to validate false identify in a stealthy node behaviour as it gives a normal impression and in case of route fabrication they modify the routing path which leads a high number of packet loss. The DAKA provides a Secure Route Discovery Mechanism and data routing through a privacy and certificate authentication methodology. **Findings:** We evaluate the proposed approach by measuring Packet Delivery Ratio, Avg. End-to-End Delay, Control Overhead and Packet Drop Ratio with varying the number of malicious nodes in a fixed number of nodes and traffic. **Application/ Improvements:** The simulation experiment result shows successfully alleviation of the malicious nodes and achieves the needed performance.

Keywords: Authentication, MANET, Prevention, Privacy, Stealthy Attacks

1. Introduction

The security in mobile ad-hoc networks is a key concern for basic functionality on the network. The availability of "network services", "data confidentiality" and "integrity" can be accomplished by ensuring that security problems are met. MANET suffers from security attacks because it has features such as "open media, dynamic topology changes, lack of central monitoring and management, collaboration algorithms and clear defence mechanisms". These features have transformed the battlefield circumstances of MANET in opposition to security threats. MANET works with no centralized management where nodes communicate with each other based on mutual trust. Because of this nature, MANETs can take advantage of by intruders inside the network. Using wireless links makes MANET more vulnerable to attack, allowing attackers to get within the network and easily access in progress communications[1–3]. Mobile nodes inside the range of the wireless link can be peeked or join the network.

However, the "open environments", "rapid deployment methods" and "hostile environments" where wireless networks can be deployed are vulnerable to widespread attacks on equal control and data traffic. In addition, several wireless networks, such as "sensor networks" are primarily resource limited in terms of energy and bandwidth. Therefore, all security protocols must adhere to these constraints. Traffic control attacks include "worm holes", "rushing" and "Sybil attacks"[11–13]. The main remarkable data traffic attacks are "black hole", "selective forwarding and delaying". A malicious node either completely or selectively deletes data or delays forwarding and the attacker hopes that the packet is false. These attacks can interfere with route configuration and interfere with network connectivity, which can seriously degrade data functionality or degrade network functionality.

*Author for correspondence

The encryption mechanism alone cannot prevent these attacks. This is because many attack, such as wormholes and rush attacks, can be initiated without accessing the encryption key or violating the encryption checks. To alleviate such attacks, various researchers used "behaviour-based detection" concepts to observe the behaviour patterns of neighbouring nodes and display uncharacteristic patterns. The conception of behaviour is associated with communication performance such as packet transmission or non-communication activities such as reporting of detected data. Common examples are "behaviour-based detection" are "Local Monitoring"[9,10,14]. In local monitoring, the node oversees a portion of the incoming and outgoing traffic to and from neighbouring nodes. This takes advantage of the open broadcast character of wireless communications. Several types of verifying are performed locally on experiential traffic to determine malicious behaviour.

For instance, a node can make sure if its neighbouring node is forwarding packets to the accurate next hop node contained by a satisfactory delay range. If a system that reaches a familiar observation is important, the detection node starts the distributed protocol to advertise the alert. This template invokes an existing approach that complies with "Baseline Local Monitoring" (BLM). Many protocols have been constructed on BLMs for intrusion detection[15,16] and have established inter-node reliability and reputation to establish secure routing. Protocols[15,17,23].

In this paper, we evaluate the DAKA (Distinct Authentication Key Approach)[5] for confidential packet loss and power consumption attacks in previous researches related to personal information access. In stealth packet deletion, an attacker accomplishes the purpose of preventing a packet commencing reaching its destination by malicious action at the intermediate node. However, malicious required to monitor the participation of local neighbourhoods in the right area of the broadcast packet to the next hop, it gives the impression that the necessary action will be taken. Finally, I would hop on or hop class at the end of these attacks can be applied to verify the packets. Bandwidth due to resource constraints and energy, a huge amount of traffic will be accepted or recognized by a multihop ad-hoc network of wireless networks[2,3,8]. This is especially true for more common data traffic or broadcast control traffic than rare unicast control traffic. Both approaches perform two basic preventive functions in MANET.

2. Background Study

In wireless network "Dynamic topology", "distributed operations" and "resource constraints" are some of the unique features that exist in ad-hoc networks and unavoidably raise the vulnerability of those networks. Many attributes can be utilized to classify attacks in ad-hoc networks. For example, it can view an attack's behaviour either manually or actively, view the source of the attack as external or internal and view the number of intruders as single or multiple. Over the past few years, researchers have been strongly researching a variety of mechanisms to make certain the security and control of data traffic on wireless networks. These methods may be broadly classified into "authentication" and "integrity services", protocols that depend on path diversity protocols, which utilize specialized hardware, protocols which require a precise recognition or utilize of statistical methods and protocols that do not consider neighbouring communication.

The path diversity technology improves path robustness by first discovering multipath paths and using paths to make available redundancy in data transmission among source and destination[7,8]. Data were coded and separated into several shares, sent to the destination by dissimilar routes. This method works well for a well-connected network but does not present sufficient path diversity for the rare network. In addition, much of this plan is costly for wireless networks with limited resources appropriate to data redundancy. In addition, these protocols may be susceptible to path discovery attacks that prevent the discovery of non-adversarial routes, such as "Sybil attacks".

To identify malicious behaviour associated with a selective drop of data, the proposed technique relies on the explicit acknowledgment of received data using the same channel or out-of-band channel[22]. This method allows detecting the deleting of secret packets at the end point. However, this method should be complemented by other techniques for inducing high communication overhead and for diagnosing and isolating malicious nodes. A natural extension is to reduce the control message overhead by reducing attack frequency to 1 in all N data messages. However, this can delay the detection of the intruders, which can cause serious damage. Some researchers utilize statistical methods to detect wormhole attacks[11].

A common drawback to utilize of such protection mechanisms as proposed in[11,17,18] is that these mecha-

nisms are not lightweight. It is not applicable to small mobile devices such as individuals established in ad-hoc networks, so using these techniques can reason more problems than can be solved. In excessive cases, this is apparent since the system is not attacked, but it is too expensive to utilize the technology. Also, as we described in the work, encryption immune technology can be exploited by attackers, where "DoS attacks" are especially important.

2.1 Stealthy Attacks

The "stealthy Attacks"[4,6] consist of two major variety of attacks. In the first type of attack, an attacker wants to disconnect the network regardless of whether it means a regular separation on the network or isolates a particular node. Associated attacks are not dividing the network, but degrading the performance of the network worldwide or locally. A distinguished "Denial of Service" (DoS) attack is an attack with the identical goal. In generally such attacks, the intruders send a huge amount of traffic to the victim from the set of nodes it controls. This allows an attacker to consider attacks that do not necessitate controlling the node but simply communicates the routing information of the truthful node to force an honest message to be interrupted. Thus, in a similar spirit to that performed in[7], the manipulated node does not know that it has intervened in the attack. Described how an attacker could change the behaviour of a node by tricking the routing table into incorrectly modifying it. Given that there is little risk of an attacker being exposed during this action, this attack is a covert attack of the same term as a common DoS attack.

The second type of stealth attack, intruders block traffic routing information selectively modifies the infected node. This was the first type of attack traffic analysis can be used to choose stealth routers "disappeared" which can be used selectively filter packets, which can be combined. "Hijacking attacks" routing protocols are done away with to avoid exploitation and messages. In other words, the end of the transmission range of the victim to the attacker eavesdropping on the type of traffic through the damaged end of the wire to take, where the transmission range of the victim is having that out.

In all of the above types of attacks, the intruders' objective is not only to achieve the attack successfully but also to perform the attack in such a way as to hide their presence and location to the maximum extent possible with minimal effort. From an offensive point of view, stealth attack detection requires far more energy and is more vulnerable to an attack that is superior. In turn, the routing protocol that is immune to stealth attacks which mean that it is better than not. In this view, we proposed authentication mechanisms[5] stealth attack techniques that can be used to enhance the study protocols.

2.2 Previous Prevention Approaches

In general, it has been widely researched to protect the network and especially to route it over the network. However, to date, mainly arguments focus on traditional settings for static wired networks. As indicated out in[18–21], mobile and especially ad-hoc networking features introduce the ability to mitigate attackers as well as truthful users.

The problem of trust in ad-hoc networks has been investigated by several researchers[8,9,14,15]. They all utilize the "Dempster-Shafer belief theory" to integrate indirect information to make a node's reputation score. Many "reputation-based approaches "undergo from poor protection in opposition to voting stuffing, in which a malicious node praises another malicious node or compliments a malicious mouth, a malicious node that implies a legitimate node[1–3]. All "reputation-based approaches" are affected by the behaviour of a node that is functioning correctly but that provides incorrect information about other nodes. Moreover, all approaches can suffer from non-convergence behaviour. Thus, the reputation of an excellent node remains low, or the reputation of a malicious node rises abnormally.

The first step in protecting the network from attacks is to understand the nature of the attack and classify it in relation to how it is performed. High-level discussion of "reliability", "integrity" and "network availability" in a variety of confidentiality issues and explains the various attack scenarios. Another example of this approach is operations[9,11,13] that contain brief descriptions of attacks against routing tables such as "black holes" and "overflow resources". Other issue, such as "digital signatures" describes how to use standard encryption techniques. The routing information for the data traffic is based on the assumption that in the same way that you can protect. Similarly[18] and [24] and a unified view of threats to describe the techniques useful in the field of cryptography. Thus, they are "mobile enemy", "spoofing" and others describe dealing with known techniques.

In[4], the author discusses "Stealthy Attacks on Wireless ad-hoc Networks: Detection and Countermeasure" (SADEC) that are built through local monitoring and can mitigate the types of stealthy attacks. SADEC's detection technology includes two high-level steps. First, a safety tip that maintains routing information is collected during the next hop. Secondly, each neighbour to add a test of responsibility. Under the second method, three attacks, a neighbour node forwarding node relative to the amount of traffic generated by that node has a different view that really reveals. So all the neighbours cannot believe it's a hop broadcast. In essence, block or transmit power control of security in the corners or along the edges of the comparator can be used to hide the behaviour from a required number. For example, there is a packet to the next hop node and security will see it. In this case, the detection is not done. SADEC is suffering from the above disadvantages.

DAKA ("Distinguished Authentication Key Approach")[5] is used to evaluate the probability of preventing malicious nodes from dropping through route creation and false identification attacks. In all modes of covert packet deletion, the malicious intermediate node achieves the same goal as deleting the packet. However, none of the protection nodes that utilize BLM become wiser due to work. In addition, legitimate nodes are charged for alleged packet loss. The approach DAKA provides modification and secure communication of existing "AODV routing protocols"[25] to solve MANET security problems. Each path to a destination has a unique key that performs a private communication. Secure information with a unique private key for each path is a new contribution of the DAKA proposal and a secure communication mechanism for messages and binding provides binding data that uses symmetric and asymmetric encryption in routing. This ensures data routing by using different unique private keys generated for each path during the routing process to prevent two important stealth attacks.

3. Prevention of Stealthy Attacks in MANET

This section describes the "Distinct Authentication Key Approach" (DAKA) mechanism of operation to supplement existing local monitoring to detect covert packet loss caused by route authoring and misidentified attacks. The first mechanism alleviates the path generation exaggerated packet drop, while the second mechanism alleviates the node "false Identification attack" type. To detect and prevent this attack, DAKA provides secure path search and data routing are integrated with privacy to prevent "Route fabrication attacks" and "Trusted Third Party" (TTP) authentication certificates to prevent "false identification attacks". Prevention mechanisms are briefly described in the following sections.

3.1 Approaches for Preventing Route Fabrication Attack

In a packet "route fabrication attack", a malicious node reroutes traffic from its original path to reach the wrong destination. The attacker misguides the packet so that it is longer than its lifetime, causing it to be lost on the network. As a result, the source node must retransmit the lost packet, which not only increases the network overhead but also consumes more bandwidth.

In a "route fabrication attack", a malicious node will knowingly forward the packet to the next hop, causing the packet to be lost. In "Baseline Local Monitoring"[11], a node that is not in the path to the destination and receives the packet to relay sends a one-hop broadcast that discards the packet or there is no route to the destination. The authors argued that the latter case would be more expensive and dangerous because it provides a valid excuse for malicious nodes dropping packets. Therefore, some of them false accusations reproach and they can go with the first choice.

Consider an example for route fabrication scenario as shown in Figure 1, where source node *S* has to send a packet to destination D through a path *S*→*A*→*M*→*F*→*D*. But when a node sends a packet to the *M* malicious node that assumes that is projected onto a daughter, but it just sends the package to the node *D*, which does not have a path to the target *D* in the final, so just fell node *D* in this package. This result concludes firstly as, "a node *M* successfully discard the packet because all packets of *M* have been forwarded successfully" and secondly "the legitimate node *D* of the node drops the packet which is classified malicious".

During data communication, an intermediate node to reduce output by modifying the data packet information can inject a false path. Daka when routing data packets using a unique secret key by encrypting the data packet handles the changes. Acknowledgment of the source node and the destination node transmits the data pack-

ets to create messages that suggest a unique secret key. The DAKA prevent the route fabrication with a secure path discovery node, where a node N creates a privacy key using DH algorithm as P_{SKey} and create a message signature using a hash algorithm as $Sign_{msg}$. To broadcast message a secure message packet is generated using TTP authenticate public key as shown in Equation 1.

$$S_{msg} = Enc\left(Sign_{msg}, Msg, P_{SKey}, D_{id}, T\right)_{A_{pubkey}} \quad (1)$$

To alleviate the route fabrication attack DAKA implements a secure route discovery and data routing. It implements a secure path discovery using privacy mechanism. The DAKA provide a privacy routing with extending the AODV path discovery mechanism as shown in Figure 2.

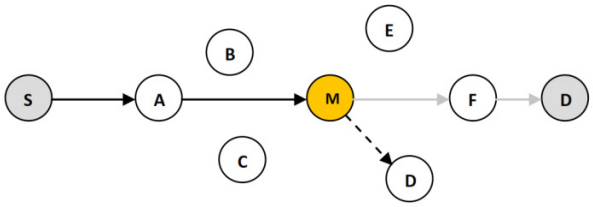

Figure 1. Route fabrication scenario.

The functionality of each method in Figure 2 is described in the algorithm 1 which implements two methods for securing route discovery and route reply for the objective to prevent the node from the route fabrication attack. The activities it performs by the intermediate and destination node on receiving the secure privacy message during route request shown in Figure 3.

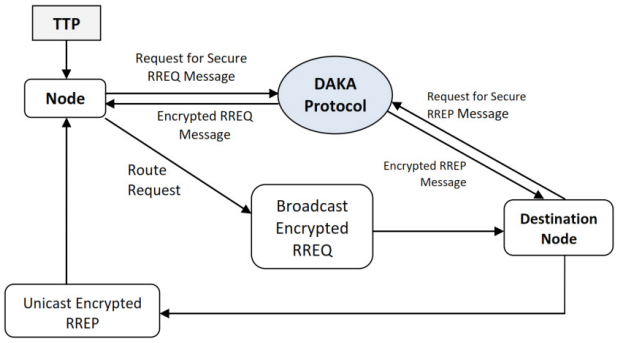

Figure 2. DAKA secure route discovery mechanism.

In data routing method data packet amendment is the major issue. During data transfer, it is always achievable that an intermediate node can apply a false path editing information packets to degrade throughput. DAKA prevents this modification of data packets by encrypting data packets using different privacy secret keys, PS_{Key}. It is used both data sending and also for delivery acknowledgment messages. Another issue in data routing is data packet dropping. This can affect network performance is nor-

Algorithm 1: *DAKA Secure Path Discovery*

Source Node, SN→ *RouteRequest(SN)*
Init *Path[] = SN.*

Method1: RouteRequest(N)
//The following steps is performed by SN before broadcasting message
Privacy Key using DH algorithm → P_{SKey}
Msg signature using Hash algo, $Enc(Msg) \rightarrow Sign_{msg}$
Secure Broadcasting msg using A_{pubkey},
$Enc([Sign_{msg}, Msg, P_{SKey}, D_{id}, Path, T])A_{pubkey} \rightarrow E_{msg}$
Broadcast E_{msg} to all neighbouring nodes as *R.*

//The following steps are performed by Intermediate Nodes
while $R_{id} \neq D_{id}$ ***do***
Decrypt receive msg using A_{pvtkey},
$Dec([Sign_{msg}, Msg, P_{SKey}, D_{id}, Path, T])A_{pvtkey} \rightarrow D_{msg}$
Msg signature using Hash algo, $Enc(Msg) \rightarrow ISigm_{msg}$

If $VerifySignature(Sign_{msg}, ISigm_{msg}) == true$ ***and*** $Msg == 'RREQ'$ ***then***
If $R_{id} \neq D_{id}$ ***then***
Append I_{id} address to Path → $Path[SN, I_{id}]$
Secure broadcasting msg using A_{pubkey},
$Enc([Sign_{msg}, Msg, PS_{key}, D_{id}, Path, T])A_{pubkey} \rightarrow E_{msg}$
Re-Broadcast E_{msg} to all neighbouring nodes.

ElseIf $R_{id} == D_{id}$ ***then***
Store source PS_{SKey} in Destination Table.
RouteReply(D).
End if
End if
End while

Method2: RoutReply(D)

Privacy Key using DH algorithm → P_{DKey}
Msg signature using Hash algo $Enc(Msg) \rightarrow Sigm_{msg}$
Secure Reply message using A_{pubkey},
$Enc([Sign_{msg}, Msg, P_{DKey}, S_{id}, Path, T])A_{pubkey} \rightarrow E_{msg}$
Send E_{msg} to the node in *Path.*

while $R_{id} \neq S_{id}$ ***do***
Decrypt receive message using A_{pvtkey},
$Dec([Sign_{msg}, Msg, P_{SKey}, S_{id}, Path, T])A_{pvtkey} \rightarrow D_{msg}$
Msg signature using Hash algo, $Enc(Msg) \rightarrow ISigm_{msg}$

If $VerifySignature(Sign_{msg}, ISigm_{msg}) == true$ ***and*** $Msg == 'RREP'$ ***then***
If $R_{id} \neq S_{id}$ ***then***
Read Next Node from *Path* [] → $Next_{Hop}$
Send E_{msg} to the $Next_{Hop}$
ElseIf $R_{id} == S_{id}$ ***then***
Store destination Privacy Key(P_{DKey}) → *RoutingTable*
End if
End if
End while

Figure 3. Algorithm to prevent from route fabrication attack.

mal behaviour for malicious ends. To handle this kind of attack, not only in our opinion, reliable and TTP-certified terminals and ensures that participate in the communication process.

3.2 Approach for Alleviating False Identification Attack

In a false identity attack, a node cannot identify a legitimate node, it can pass the responsibility of sending to a node close to the sender and the cause of the packet loss may be a damaged node in the path between the sender and the receiver. This form of attack, the attacker uses a packet drop two malicious nodes. Sender airspace is near an end. The other end of the caller to the next hop. A malicious node is the first node can be decomposed externally or internally and the latter must be an inside corrupted node.

Consider the false identification scenario shown in Figure 4. The source node S wants to sends a packet to *D* via node *A* and *M* is malicious near to node *S*. The False Identification attack involves two malicious nodes. One is the next hop of the sender, *A* and another one is spatially close to the sender *M*, which is allowed to utilize *A*'s identity to transmit. Due to this false identification *S* transmit the packets to *M* instead of *A*. In such case *D* will never receive the packet as *D* is out of range of *M*. Again, the consequences of this attack conclude two cases: 1. "The packet has been successfully dropped without detection" and 2. "The node A is accused of dropping packets".

Establishing a secure connection between mobile ad-hoc network nodes is the hardest part. Due to the difficulty and nature of mobile ad-hoc networks, it cannot utilize predefined architectures for security. The majority of work related to privacy and key distribution has not been well addressed, in the most secure routing protocol. Security associations and the work of the previous secure routing protocols related to key distribution are not at their best. One simple solution, the presence of security associations between source and target nodes is described in[22] and "group key exchange" is described in[24]. A group key is based on a strong shared key but in the case of high mobility behaviour where nodes join and leave very regularly affects the mechanism. In[2,3,16] describes a further process security associations between nodes that utilize asymmetric cryptography, where any node in the network can issue a certificate to the new nodes. This is a powerful approach in the sense that it has no single point of failure in the network. But it still can have attacks of vulnerability to verify the new node and a certificate is risky if malicious nodes are already in the network.

In DAKA mechanism, which has a primary security association between the nodes distributes "TTP certificates" to have a secure identification. But to get confirmation from a Trusted Third Party (TTP) and it must be loaded into each node before it connects to the network. It will be an offline process in which each node must obtain their certificates from TTP. In this approach, if a node is trying to illegally acquire an unacceptable certificate can trap and removed effortlessly.

The certificate given by the *TTP* for a node *N* will be consists of a TTP authorized public and private key as A_{pubkey} and A_{pvtkey} and a node public and private key as N_{pubkey} and N_{pvtkey}. The TTP certificate of a node represented as:

$$A_{cert} = A_{pubkey}, A_{pvtkey}, N_{pubkey}, N_{pvtkey}$$

This certificate is valid for all nodes of the network that we have received, assume that before entering the network. The process of obtaining certification, the internal node provides basic identity prevents malware, prevents attacks and form identification error. Deleting data packets that can affect network performance malicious nodes is a common behaviour. To handle this type of attack, the DAKA mechanism requires that a trusted CA authentication node participates in the communication process.

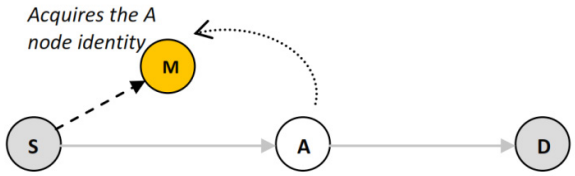

Figure 4. False identification illustration scenario.

4. Experiment Evaluation

The evaluation of our proposal is that we assume that both types of malicious nodes in the internal and external. However, most of the nodes in the network are a trustable CA certification acquisition we have to assume that the message data and the protection of the internal network against external attacks and symmetric cryptography to protect encryption node utilize of public key cryptography.

We experimentally evaluate the performance of our program using the simulator to simulate using Glomosim.

It is operated by a wireless protocol simulation environment provides a scalable and parameter. We compare the performance of DAKA[5] with AODV[25], SADEC[4] for evaluation analysis. Table 1 shows the simulation configuration parameter values.

We complete the experiment support on the Table 1 for a phase of 600 seconds. The simulation is performed in a Random Waypoint behaviour model where each node is randomly placed during the pause time, randomly selecting a new position and moving at a speed between 0-10 m/s. We run the simulation by changing the number of malicious nodes five times utilizing the configured values shown in Table 1. For evaluating the protocol routing we have occupied 50% of nodes as traffic as "source-destination pairs" at Constant Bit Rate (CBR) flow of 4 data packets per seconds and each packet size is 512 bytes in size. We evaluate the protocol by measure "Packet Delivery Ratio", "Avg. End-to-End Delay", "Control Overhead" and "Packet Drop Ratio" with varying the malicious nodes from 5 to 25 nodes with a fixed number of nodes and traffic.

Table 1. Configuration parameter values

Configuration	Parameter Values
Simulation Time	600s
Simulation Area	1000m X 1000m
No. of Nodes	50
Mobility	RWP
Mobility Speed	0 to 10 m/s
Pause Time	30s
Packet Size	512 bytes
CBR Rates	4 pkts/sec
Malicious Nodes	5,10,15,20,25

4.1 Results Analysis

- **Packet Delivery Ratio:** Packet Delivery Ratio (PDR) defines the "total number of data packets received and the total number of data packets generated for transmission". The PDR defines the throughput of the protocol.

$$PacketDeliveryRatio = \frac{\sum ReceivedPackets}{\sum PacketsOriginated}$$

Figure 5 shows the Packet Delivery Ratio for AODV, SADEC and DAKA. It describes that increasing the number of malicious nodes in the network impacts the protocol throughput. Packet Delivery Ratio of DAKA outperforms over AODV and SADEC due its secure mechanism does not allow any node to intrude. But the Packet Delivery Ratio of the protocols resulting low when increasing the number of malicious nodes. The performance of DAKA remains improved than AODV and SADEC with increases the malicious nodes is due to effective prevention leads in compared.

- **End-to-End Delay:** End-To-End Delay calculated as the time between the transmissions of a data packet from a source to the destination.

$$End-to-EndDelay = \frac{\sum AverageEnd-to-EndDelay}{No.\ ofNodes}$$

Figure 6 describes Avg. end-to-end delay of AODV, SADEC and DAKA protocol. It illustrates that DAKA it attains less end-to-end delay in compares to AODV and SADEC. An increase in the number of malicious nodes leads to high delay in AODV and SADEC in compare to DAKA. The increment of delay in AODV and SADEC is increased due to the malicious nodes misrouting or identity falsification causes a number of packet loss, whereas DAKA preserves less end-to-end delays due to it effective prevention against these attacks.

- **Control Overhead:** Control Overhead is "calculated based on the total number of control packets initiated and delivered by the protocol during the entire communication process".

$$ControlOverhead = \sum NumberofControlPackets$$

Figure 7 describes the Control Overhead between AODV, SADEC and DAKA protocol. It was experiential that DAKA attained higher overhead in compares to SADEC but lower to AODV. All protocols show the increase in overhead as the number of malicious nodes in the network increases. The increase in DAKA overhead is appropriate to the introduction prevention mechanism which increases the number of control packets between nodes. Due to frequent monitoring of neighbours and verification of identities for their identities, they represent a higher overhead compared to SADEC.

- **Packet Drop Ratio:** The rate at which "packets are dropped computed based on the total number of packets dropped by the protocol during the entire communication process".

$$Avg.PacketDropRatio = \frac{\sum NumberofPacketDropped}{No.ofNodes}$$

Figure 8 describes the Avg. packet drop ratio among AODV, SADEC and DAKA protocol. It was observed that DAKA had lower packet drop ratio in compares to AODV and SADEC. All protocol packet drop rates increase as

the number of malicious nodes in the network increases. The reduction in packet drop rates at DAKA is due to efficient preventive maintenance between nodes that minimizes intrusions and improves network lifetime and throughput.

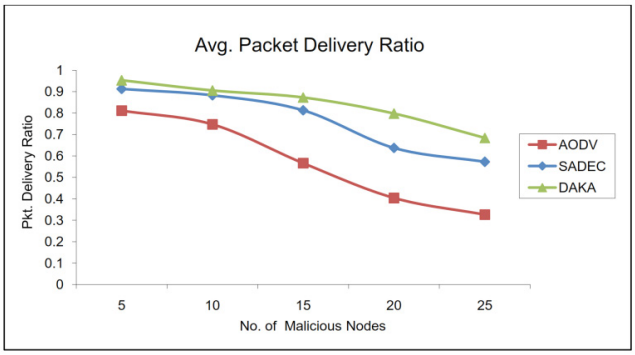

Figure 5. Packet Delivery Ratio.

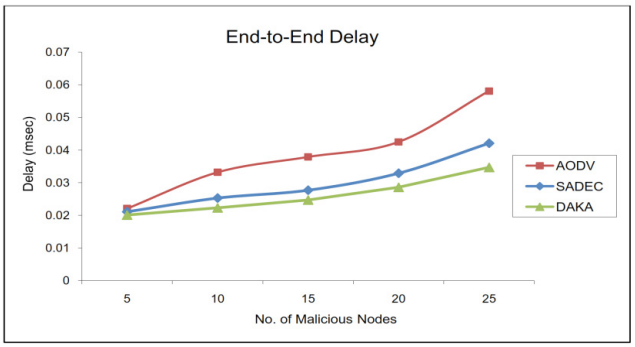

Figure 6. Avg. End-to-End Delay.

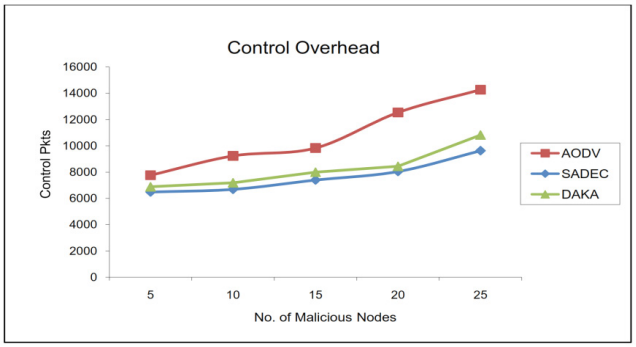

Figure 7. Control Overhead.

5. Conclusion

We utilize a "Distinct Authentication Key Approach (DAKA)" privacy mechanism for mobile ad-hoc networks that protects routing mechanisms from internal and external attacks and also prevent from "stealth attacks". We analyze two types of stealthy attacks: "Route Fabrication Attack" and "False Identification Attack." It utilizes a public key cryptography mechanism to Route Fabrication Attack through secure route discovery messages and prevents false identification attacks through secure TTP certificates. DAKA's experimental evaluation shows instantaneous throughput with optimal Control Overhead and end-to-end delay of various malicious node changes. The effect of packet drop increases with the malicious nodes but DAKA efficiently handles the intruders based on the secure message communication and unique TTP identity. In the future cryptographic process can impact any regulation even more important parameter to evaluate the timing of the surge, and the simulation from motion-effects of mobile ad-hoc network performance have a greater impact that must be observed, therefore, the future of work mobility link failure, the revision process to handle the protocol can increase.

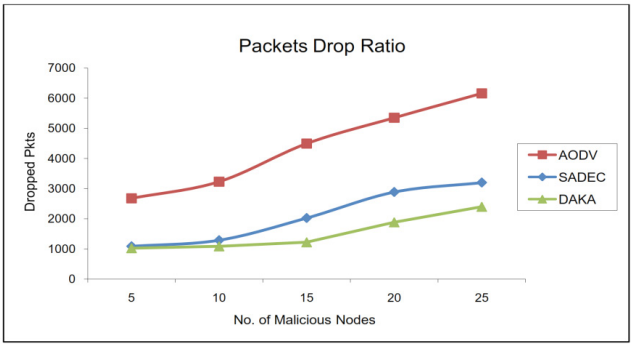

Figure 8. Avg. Packet Drop Ratio.

6. Reference

1. Khana A, Imranb M, Abbasa H, Duradb MH. A detection and prevention system against collaborative attacks in mobile ad-hoc networks. Elsevier Future Generation Computer Systems. 2016; 68:416–27. Crossref
2. Gharib M, Moradlou Z, Doostari MA, Movaghar A. Fully distributed ECC-based key management for mobile ad-hoc networks. Elsevier Computer Networks. 2016; 113:269–83. Crossref
3. Smith HJ, Wetherall J, Adekunle A. SUPERMAN: Security Using Pre-Existing Routing for Mobile Ad-hoc Networks. IEEE Transactions on Mobile Computing. 2017 Jan; PP(99):1–1.
4. Khalil I, Bagchi S, Shroff N. LITEWORP. A Lightweight Countermeasure for the Wormhole Attack in Multihop Wireless Networks. Proc International Conf Dependable Systems and Networks (DSN '05); 2005. p. 612–21. Crossref

5. Yan J, Ma J, Li F, Moon SJ. Key pre-distribution scheme with node revocation for Wireless Sensor Networks. Ad-hoc and Sensor Wireless Networks. 2010; 10(2/3):235–51.
6. Angu M, Anand S. Detection and avoidance of gray hole attack in mobile ad-hoc network. Indian Journal of Science and Technology. 2016 Dec; 9(47):1–6. Crossref
7. Boppana RV, Su X. On the effectiveness of monitoring for intrusion detection in mobile ad-hoc networks. IEEE Transactions on Mobile Computing. 2011 Aug; 10(8):1162–74. Crossref
8. Xiao Y, Rayi VK, Sun B, Du X, Hu F, Galloway M. A survey of key management schemes in Wireless Sensor Networks. Computer Comm. 2007 Sep; 30(11/12):2314–41. Crossref
9. Wu Y, Marmol FG, Al-Duba A. Introduction to advances in trust, security and privacy for wireless networks. Proceeding EURASIP Journal on Wireless Communications and Networking; 2013. p. 287–88. Crossref
10. Huang Y, Lee W. A cooperative intrusion detection system for ad-hoc networks. Proc ACM Workshop Security of Ad-hoc and Sensor Networks (SASN '03); 2003. p. 135–47. Crossref
11. Defrawy KE, Tsudik G. ALARM: Anonymous Location-Aided Routing in Suspicious MANETs. IEEE Trans Mobile Comput. 2011; 10(9):1345–58. Crossref
12. Kumar V, Das ML. Securing Wireless Sensor Networks with public key techniques. Ad-hoc and Sensor Wireless Networks. 2008; 5(3/4):189–201.
13. Ganeriwal S, Balzano LK, Srivastava MB. Reputation-based framework for high integrity sensor networks. ACM Trans Sensor Networks. 2008 May; 4(3):1–37. Crossref
14. Babu DVS, Reddy PC. A distinct authentication key approach for privacy and high performance in MANET. International Journal of Computer Networks and Security. 2015 Feb; 25(1):1–24. ISSN: 2051-6878.
15. Lacuesta R, Lloret J, Garcia M, Penalver L. A secure protocol for spontaneous wireless ad-hoc networks creation. IEEE Transactions on Parallel and Distributed Systems. 2013 Apr; 24(4):629–41. Crossref
16. Jain S, Shastri A, Chaurasia BK. Analysis and feasibility of reactive routing protocols with malicious nodes in MANETs. Proceeding International Conference on Communication Systems and Network Technologies; 2013 Apr. p.1–5. Crossref
17. Liu K, Deng J, Varshney PK, Balakrishnan K. An acknowledgment-based approach for the detection of routing misbehaviour in MANETs. IEEE Trans Mobile Computing. 2007 May; 6(5):536–50. Crossref
18. Marti S, Giuli TJ, Lai K, Baker M. Mitigating routing misbehaviour in mobile ad-hoc networks. Proc of the 6th Annual International Conference on Mobile Computing and Networking; 2000 Aug. p. 255–65.
19. Khalil I, Bagchi S. Stealthy attacks in wireless ad-hoc networks. Detection and Countermeasure IEEE Transactions on Mobile Computing. 2011 Aug; 10(8):1096–112. Crossref
20. Arthur MP, Kannan K. Intelligent internal stealthy attack and its countermeasure for multicast routing protocol in MANET. ETRI Journal. 2015; 37:1108–19. Crossref
21. Li H, Chen Z, Qin X. Secure routing in wired networks and wireless ad-hoc networks. Department of Computer Science: Univ of Kentucky; Term-paper. 2003. p. 1–10.
22. Pakzad F, Rafsanjani MK. Intrusion detection techniques for detecting misbehaving nodes. Published by Canadian Centre of Science and Education. 2011 Jan; 4(1):1–7.
23. Huang YA, Fan W, Lee W, Yu PS. Cross-feature analysis for detecting ad-hoc routing anomalies. Proc of the 23rd International Conference on Distributed Computing Systems (ICDCS); 2003. p. 478–89. PMCid: PMC1241431.
24. Liu D, Ning P. Establishing pair-wise keys in distributed sensor networks. Proc ACM Conf Computer and Comm Security (CCS '03); 2003. p. 52–61.
25. Perkins CE, Royer EM. Ad-hoc on-demand distance vector routing. Proc Second IEEE Workshop Mobile Computing Systems and Applications (WMCSA '99); 1999. p. 90–100. Crossref