Biomedical Research 2018; 29 (9): 1743-1749 *ISSN 0970-938X*
www.biomedres.info

Preventing clone attacks using dynamic cryptography in MANETs.

Saravanan R[1*], Ilavarasan E[2]

[1]Department of Computer Science and Engineering, Manomanian Sundaranar University, Tirunelveli, Tamil Nadu, India

[2]Department of Computer Science and Engineering, Pondicherry Engineering College, Puducherry, India

Abstract

Mobile Ad-Hoc Networks (MANETs) use anonymous routing protocols that hide node identifies and/or routes from outside observers in order to provide anonymity protection. In this attack, an adversary captures few nodes, replicates them and then deploys arbitrary number of replicas throughout the network. It is very hard to distinguish between non-compromised nodes a clone node since a clone has the same security and code information of original node. Hence cloned nodes can launch a variety of other attacks. The detection of cloning attacks is therefore a fundamental problem. The main objective of this method is to prevent clone attacks in MANETs while routing. A clone attack is launched by a malicious node by copying the configuration of a legitimate active node of current operating network. Polynomial bivariate keys are used for preventing clone attacks while routing by validating the next hop until the data reaches the destination. A polynomial key based authentication layer in AODV is used to demonstrate the clone attack prevention in the MANET.

Keywords: Mobile ad-hoc network, Clone attack, Polynomial key, Mobility, Detection.

Accepted on September 7, 2017

Introduction

Mobile Ad-hoc Networks (MANETs) fall under the most widely used communication technologies especially because of the features like mobility, dynamic infrastructure, dynamic and easy link establishment and reconfiguration [1]. The mobile devices are free to move randomly and arrange themselves randomly. The communication takes place in MANET by using multi-hop paths. Nodes in the MANET share the wireless medium and the topology of the network changes dynamically. Since the nodes are mobile, there is a chance for communication link breakage. The application areas of MANET have mostly been in critical areas where the routing performance and security is expected to be close to ideal. However, this is not achievable practically and hence strategies to achieve greater security adopt.

The primary concerned security issue in MANETs is to protect the network layer from malicious attacks and to detect and prevent malicious nodes in the communication network [2]. The security solution is important to protect both route and data forwarding operations in the network layer. Lacking any proper security solution, each malicious node tends to act as a readily available router, which will solely disturb the network operation from correct delivering of the packets and the malicious nodes can give stale routing updates or drop all the packets passing through them.

One important mechanism to detect clone attacks is the time domain detection. Time is divided into equal length intervals and the time intervals are associated with the challenge. Trusted node broadcasts the challenge to every node in the network initially. Based on the one-way property of hash function, it can easily verify the authenticity by using any of the previously verified challenge of the preloaded one. Also space domain detection is used for detecting node replication attacks. This scheme consists of two phases: the local check phase and the local witness check phase. The local check is the phase when two needs meet each other and exchange information according to the local information exchange. The witness nodes record the inevitable information during exchanging the information in the node to node. Once the nodes meet each other, they exchange the recorded information about identity.

Clone attack or node replication attack is a severe attack in MANET [3]. In this attack an adversary captures only a small number of nodes replicates them and then deploys arbitrary number of replicas throughout the network. It is very hard to distinguish between non-compromised nodes a clone node since a clone has the same security and code information of original node. Hence cloned nodes can launch a variety of other attacks. Detection and prevention of cloning attacks in a mobile ad hoc network is a fundamental problem and cannot be easily handled [4]. Most of the existing protocols expose the following limitations: high performance overheads, necessity

of central control, unreasonable assumptions, lack of smart attack detection etc.

The polynomial key verification is used to differentiate the nodes within the network whether they are replicas or legitimate nodes. On encountering malicious nodes, data is sent through alternate routes to reach the destination. The nodes in the network operate with greater security and hence there is greater packet reception lesser loss in the network. Also by routing through legitimate nodes the energy drain is reduced in the network the reason being there is greater energy remaining in PK-AODV.

Related Work

SAR (Secure-Aware Ad Hoc Routing protocol), using AODV, It proposed encryption and decryption process using a common key [5]. SAR defines a level of trust as a metric for routing and as an attribute for security for routing. The main drawback with SAR protocol is whenever the levels of security rise; it needs different keys for different levels, thereby increasing the number of keys [6]. SEAD is a secure efficient ad hoc distance vector routing protocol. It uses one-way hash function without the usage of asymmetric cryptographic mechanism. Authentication is used by this mechanism to differentiate between malicious and non-malicious nodes, and reduces resource consumption attacks launched by malicious nodes. It can overcome DoS, many types of routing attacks and resource consumption attacks also avoid routing loops. The drawback lies whenever the attacker uses the same metric and sequence number used for authentication were same by the recent update message and updates with new update message. ARAN (Authenticated Routing for Ad Hoc Networks) based on cryptographic certificates which overcome all types of attacks in the network layer [7]. ARAN provides authentication, integrity and non-repudiation. However, this protocol mechanism is quite robust against attacks, and is mainly based on prior security coordination among nodes which cannot be correctly assures at all times [8]. Drawbacks for any protocol to be used in the WSN-resource-constrained environment also vulnerability is an issue. Randomized, Efficient, and Distributed (RED) protocol proposed detection of node replication attacks, and self-healing. Detecting replication attacks is a nontrivial problem in MANETs due to the challenges resulted from node mobility, cloned/compromised node conspiracy, and the large number and wide spread replicas [9]. Existing approaches either fails in mobile environments due to the limitations caused by local views or their dependence on invariant claims such as location and neighbour list, or are constrained by the number and malicious activities of the replicas. Detecting Replica Attacks in Mobile Ad Hoc Networks proposed two replication detection schemes (TDD and SDD) to tackle all these challenges from both the time domain and the space domain [10]. The authors have proved that TDD and SDD provide high detection accuracy and excellent resilience against smart and colluding replicas, have no restriction on the number and distribution of replicas, and incur low communication/computation overhead. Dynamic detection of node replication attack aims to detect the cloned node in the environment network. The most obvious attack in wireless sensor network is node replication attack [11]. This attack the nodes are replicated manually based on their id and key values. Cloned node or adversary promotes the node key or id of the legitimate node, creates more replicas of the particular node in the current network with the same id and also this node may cripple the entire network. It detects clone replication attack in dynamic way and to detect the replicas in mobile wireless sensor network [12]. Existing schemes rely on fixed sensor locations and hence do not work in mobile sensor networks, where sensors are expected to move [13]. A fast and effective mobile replica node detection scheme using the sequential probability ratio test was developed [14]. The problem of replica node attacks in MANETs is tackled here. Using SPRT, this scheme detects mobile replicas in an efficient and robust manner at the cost of reasonable overheads. Executing and checking the test cases is not possible all the time in the manual testing. Therefore selecting a test case and ranking is important [15]. The objective of the test case selection is to have a better test case from a pool of test cases and assigning the rank to each test case will leads the software as an error free and which gives a good efficiency. Ranking of test cases is especially useful if a system is a having large number of test cases. Hence selecting and ranking a test case plays an important role in the software testing. Automation tools helps in design and execution of test scripts saving time and cost involved in manual testing [16].

Proposed Method

The bivariate t-degree polynomials coefficient over a finite field '*P*' is calculated by using the following formula, where *P* is a prime number to accommodate a cryptographic key. The key is calculated for the each and every link exists between the nodes.

$$F(a,b) = \sum_{0 \le i \le t}^{t} c_{ij} a^i b^j \rightarrow (1)$$

As the topology of the network changes dynamically in the MANET, the key is also calculated dynamically. It has one property $F(x, y)=F(y, x)$ and $C_{ij}=C_{ji}$.

The same key is used for the data transmission from *X* to *Y* and From *Y* to *X*. Even though the attacker compromise the node and capture the key, then introduce the malicious node with same configuration by using the compromised parameters, the rest of the normal nodes present in the network can easily identify it is a replicated node since the key of the changed dynamically.

Flat topology

The flowchart and algorithm description of PK-AODV is shown in figure below.

Figure 1 shows the operation of the nodes inside the network. All nodes are verified using the polynomial key verification process. If the nodes pass the verification, then the nodes can

continue communicating with the verified node. Otherwise, although the node id remains the same, through the polynomial key verification between the nodes 2 and 4, the node 2 is identified as clone of the legitimate node 2. Preventing the cloned attacker, the communication can be performed through an alternate neighbor of the source node. This process is continuously and consecutively performed until the data reaches the destination.

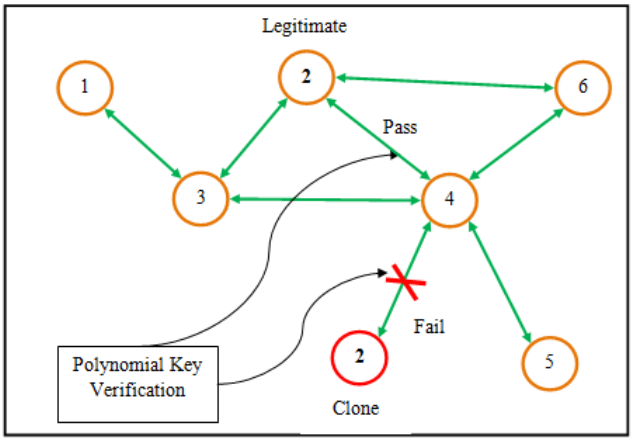
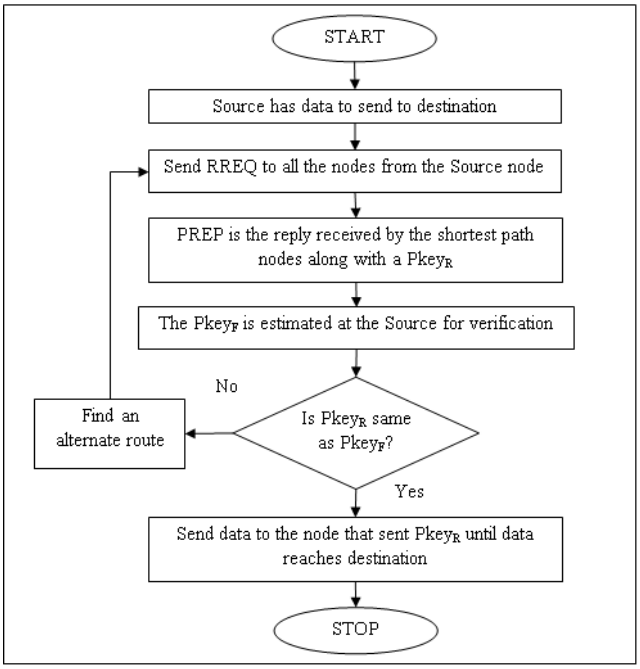


Figure 1. *Polynomial key verification between nodes.*



Hierarchical topology

The flowchart and algorithm description under hierarchical topology is described below.

If the node that detects the malicious node broadcasts information by sending malicious node ID, then the legitimate node that has the same ID may be eliminated from the routing tables of the neighboring nodes. This is a threat to the network as some of the links will be deleted although they seem to be functioning well. Hence all communicating nodes are verified hop-by-hop whether they are legitimate. This method can hence act as an efficient method to perform communication between the nodes in the network preventing the occurrence of clone attacks.

Algorithm

Set this_node = source;
{
Get neighbours(this_node);
Send request RREQ to all the neighbours(this_node);
Each node sends PREP along with the Pkey$_R$;
Source receives Pkey$_R$ and estimates Pkey$_F$;
If { Pkey$_R$ == Pkey$_F$} {
Send data this_node → next_node
Set this_node = next_node;
Goto step 1 until data reaches destination;
} else {
Skip the node and goto step 4;
}
}

Line No	Algorithm
1	For all n ϵ N {
2	BS sends Pilot signal to n;
3	n replies to BS with distances;
4	}
5	Pick a node for each region *r* ϵ G as CH {
6	If i's distance < Range(CH) { // i ϵ N
7	CH send Pkey$_F$ to node i
8	node i replies with Pkey$_R$
9	If { Pkey$_R$ == Pkey$_F$} {
10	Add node *i* to cluster *r* until max cluster size is reached
11	} else {
12	Skip i and goto step 5
13	}
14	Follow flat topology for data transfer from node to BS via CH

Simulation analysis

The simulation of the proposed system against a scenario with the attacks modelled is performed using the network simulator. The nodes in the network are verified whether malicious or not depending on the key.

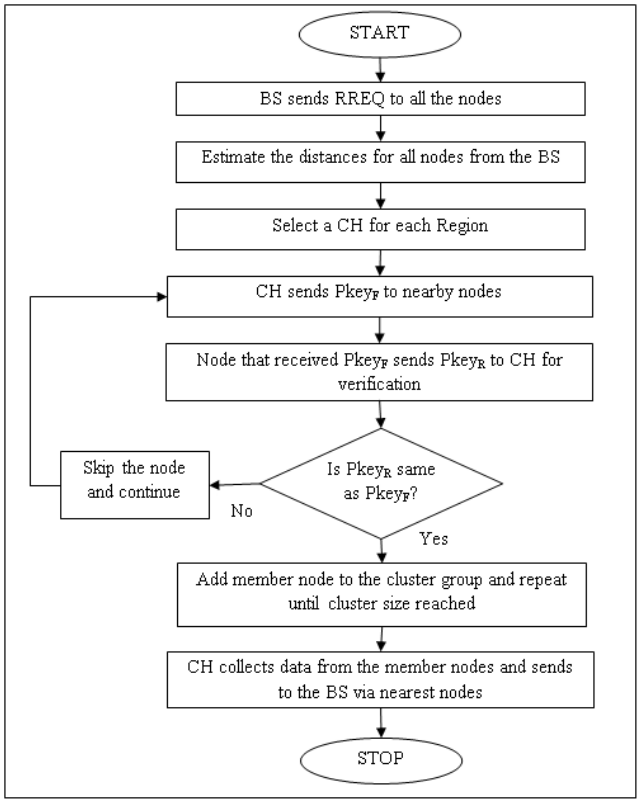
Analysis under flat topology

The working of PK-AODV is accessed in the flat topology of 30 nodes is simulated with a random number of nodes behaving maliciously during runtime. Randomly some of these nodes are replicated in the network. The malicious nodes are modeled by creation of keys other than the polynomial function but with the same id number. During hop-by-hop communication from source to destination, each node is check for the polynomial key verification and only on successful verification is the data sent across the network. When a clone attacker is encountered, an alternate path is taken by the data. The performance of this work is analysed by measuring the packet receive rate, packet loss rate, energy consumption and detection ratio. Table 1 shows the simulation parameters used for the simulation.

Table 1. *Simulation parameters used for the proposed method.*

Parameter	Value

Channel type	Wireless channel
Radio propagation model	Two ray ground
Network interface type	Wireless phy
Mac type	IEEE 802.11
Interface queue type	PriQueue
Link layer type	LL
Antenna model	Omni antenna
Routing protocol	AODV
Number of nodes	30
Simulation area	1000 × 1000 m



Packet receive rate

The packet receive rate is measured by counting the actual number of packets received over the simulation time.

PRR=(No. of packets received)/time → (2)

It can be observed from the Figure 2 that the number of packets received by the PK-AODV mechanism is greater than that of the normal AODV mechanism. This is because of the avoidance of the cloned nodes from within the regular routes while information is transferred within the network.

Packet loss rate

The total number of packets lost over the simulation time is called as the packet loss rate. The packet loss rate is defined by the Equation 3.

PLR=(Number of packets dropped)/Time → (3)

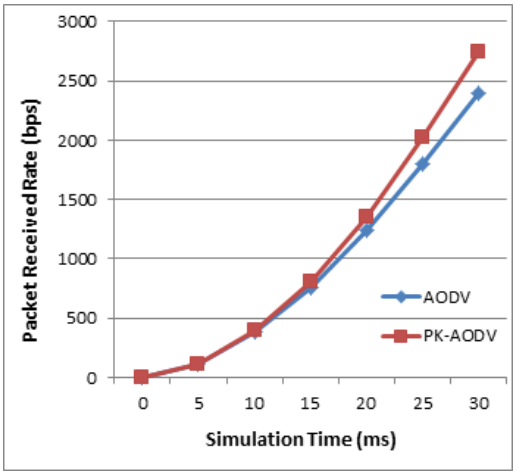


Figure 2. *Packet received rates of AODV and PK-AODV (flat).*

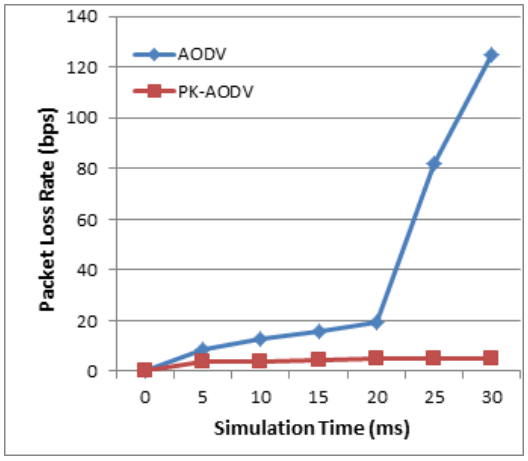


Figure 3. *Packet loss rates of AODV and PK-AODV (flat).*

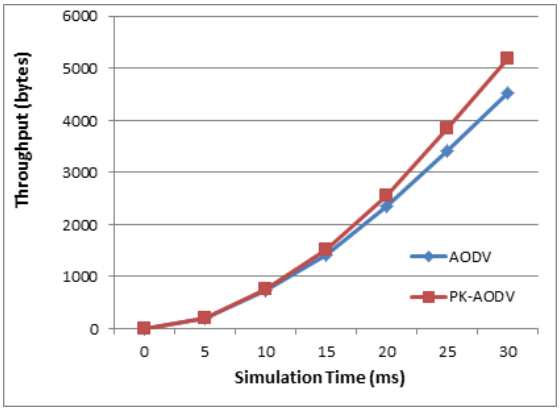


Figure 4. *Packet received rates of AODV and PK-AODV (flat).*

Figure 3 shows the comparison of the packet loss rates of both AODV and PK-AODV. The reason why the proposed method performs better than the normal AODV is that the cloned nodes cause packet loss in the network.

Throughput

The total number packet delivered by the various nodes in the entire network is called as throughput. The network throughput is given in bytes over the simulation time for both AODV and PK-AODV in Figure 4.

Residual energy

The residual energy is the energy remaining in a node and it is calculated by using the following formula in Equation 4.

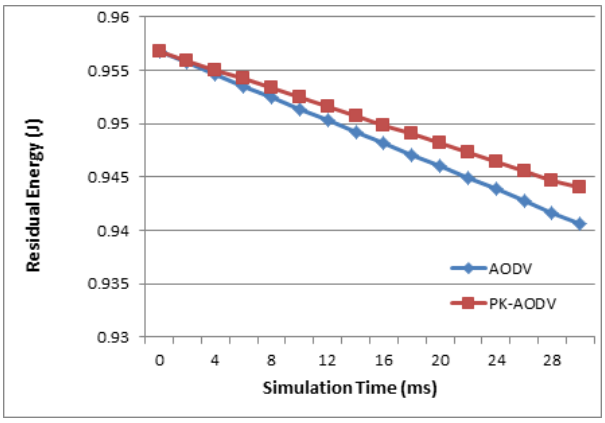


Figure 5. *Packet received rates of AODV and PK-AODV (flat).*

Average residual energy=E_T-($n \times P_T$) → (4)

Where,

E_T-Total energy

n-Number of transmission

P_T-Transmission power

Clearly, the energy consumed by the data transmission and reception processes is avoided in the PK-AODV method which is why there is greater average residual energy when compared to the AODV mechanism (Figure 5).

Analysis under hierarchical topology

The working of PK-AODV and AODV is assessed first in the flat topology in a 30-node scenario. The flat topology analysis is more like an intermediate stage of the development of the proposed protocols. Similar to the previous analysis, PDR, PLR, throughput, and residual energy are shown for PK-AODV and AODV.

Packet receive rate

The packet receive rate is measured by counting the actual number of packets received over the simulation time.

It can be observed from the Figure 6 that the number of packets received by the PK-AODV mechanism is greater than that of the normal AODV mechanism.

Packet loss rate

The total number of packets lost over the simulation time is called as the packet loss rate. The packet loss rate is defined by the Equation 3.

Figure 7 shows the comparison of the packet loss rates of both AODV and PK-AODV. The reason why the proposed method performs better than the normal AODV is that the cloned nodes cause packet loss in the network.

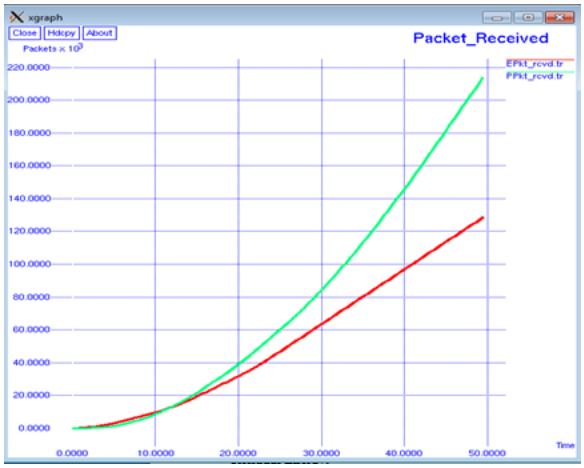


Figure 6. *Packet received rates of AODV and PK-AODV (hierarchical).*

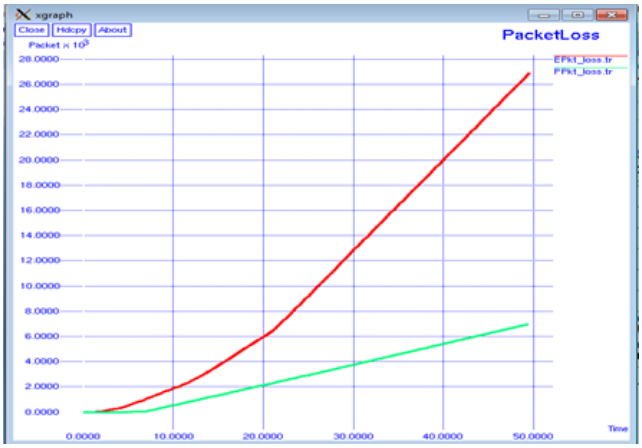


Figure 7. *Packet loss rates of AODV and PK-AODV (hierarchical).*

Throughput

The total number packet delivered by the various nodes in the entire network is called as throughput. The network throughput is given in bytes over the simulation time for both AODV and PK-AODV in Figure 8.

Residual energy

The residual energy is the energy remaining in a node and it is calculated by using the following formula in Equation 4.

Clearly, the energy consumed by the data transmission and reception processes is avoided in the PK-AODV method which

is why there is greater average residual energy when compared to the AODV mechanism (Figure 9).

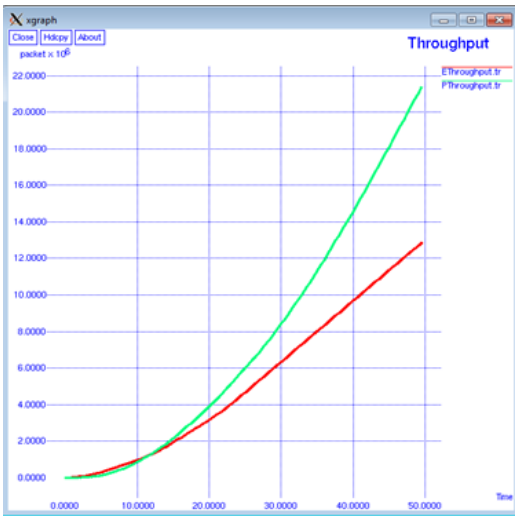


Figure 8. *Packet received rates of AODV and PK-AODV (hierarchical).*

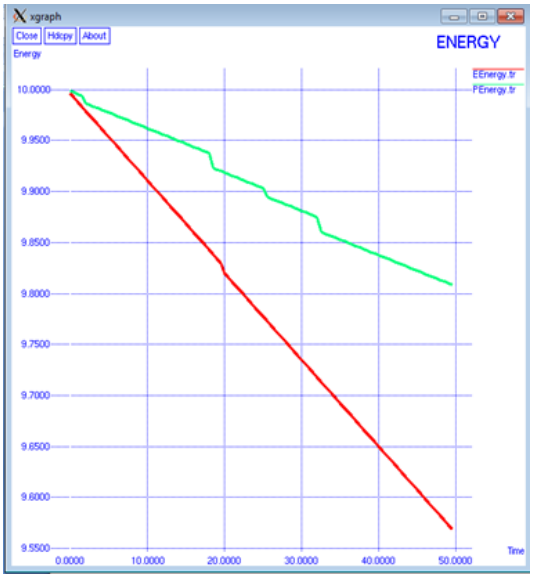


Figure 9. *Packet received rates of AODV and PK-AODV (hierarchical).*

Conclusion

The polynomial key verification is hence used to differentiate the nodes within the network whether they are replicas or legitimate nodes while communication is performed. On encountering malicious nodes, data is sent through alternate routes to reach the destination. The nodes in the network operate with greater security and hence there is greater packet reception lesser loss in the network. Also by routing through legitimate nodes the energy drain is reduced in the network which is why there is greater energy remaining in PK-AODV.

Future works aim at providing data integrity by combining PK-AODV with security algorithms. Also this mechanism can be adopted by hybrid networks by implementing the suitable integration modules, which can be done in future works.

References

1. Laura MF. Mobile networks and applications. ACM Dig Lib 2001; 6: 239-249.
2. Suresh S, Mike W, Raghavendra CS. Power-aware routing in mobile ad hoc networks. Proc Fourth ACM/IEEE Conf Mob Comp Network 1998; 181-190.
3. Manjeet S, Gaganpreet K. Surveys of attacks in MANET. Int J Adv Res Comp Sci Softw Eng 2013; 3.
4. Mauro C. Distributed detection of clone attacks in wireless sensor networks. IEEE Trans Depend Secure Comp 2011; 8.
5. Yi S, Naldurg P, Kravets R. Security-aware Ad Hoc routing for wireless networks. Proc ACM MOBIHOC 2001; 299-302.
6. Hu YC, Johnson DB, Perrig A. SEAD: Secure Efficient Distance vector routing for mobile wireless ad hoc networks. Proc 4th IEEE Workshop Mob Comp Sys Appl Callicoon NY 2002; 3-13.
7. Kimaya S, Bridget D, Brian NL, Clay S, Elizabeth M, Belding R. A secure routing protocol for Ad hoc networks. Proceedings of the 10thIEEE International Conference on Network Protocols (ICNP 02) 2002; 78-87.
8. Conti M, Di Pietro R, Mancini LV, Mei A. Distributed detection of clone attacks in wireless sensor networks. IEEE Trans Depend Secur Comp 2011; 8: 685-698.
9. Xing K, Xiuzhen C. From time domain to space domain: Detecting replica attacks in mobile ad hoc networks. INFOCOM Proc IEEE 2010; 1-9.
10. Xing K, Cheng X. From time domain to space domain: detecting replica attacks in mobile Ad hoc networks. 2010 Proceedings IEEE INFOCOM San Diego CA 2010; 1-9.
11. Sheela DP, Mahadevan G. Efficient approach to detect clone attacks in wireless sensor networks. IEEE Trans Wireless Netw 2011.
12. Balaganesh M, Nithyadhevi S. Dynamic detection of node replication attack in wireless sensor network using MANET. Int J Comp Appl 2014; 94.
13. Wen H, Luo J, Zhou L. Lightweight and effective detection scheme for node clone attack in wireless sensor networks. IET Wireless Sensors 2011.
14. Ho M. Fast detection of mobile replica node attacks in wireless sensor networks using sequential hypothesis testing. IEEE Trans Mob Comp 2011; 10.
15. Kaluri R, Lakshmanna K, Reddy T, Karnam S, Koppu S. A comparative study on selecting and ranking the test cases in software testing. ARPN J Eng Appl Sci 2016; 11: 754-757.
16. Rishab JC, Kaluri R. Design of automation scripts execution application for Selenium Webdriver and TestNG Framework. ARPN J Eng Appl Sci 2015; 10: 2.

***Correspondence to**

Saravanan R

Department of Computer Science and Engineering

Manomanian Sundaranar University

Tamil Nadu

India