AENSI Journals

Australian Journal of Basic and Applied Sciences

ISSN:1991-8178

Journal home page: www.ajbasweb.com

Secure and Cluster Based Ad-hoc Routing Using Misbehaviour Report Authentication

[1]A. Swaminathan, [2]K. Parkavi, [3]Dr. P. Vivekanandan, [4]S. Arun Rajesh

[1,2]Research scholar, Department of Computer Science and Engineering, CEG, Anna University, Chennai, India.
[3]Professor&Head,Computer Centre, Anna University, Chennai, India.
[4]Research scholar, Department of Computer Science and Engineering, Manomaniam Sundaranar University, India.

ARTICLE INFO

Article history:
Received 19 August 2014
Received in revised form
19 September 2014
Accepted 29 September 2014
Available online 12 November 2014

Keywords:
Ad-hoc, routing, cooperative, security, cluster, malicious, encryption.

ABSTRACT

An Ad-hoc network is an emerging technology that has been attracting tremendous attention from researchers. Because these networks can be deployed quickly without relying on a predefined infrastructure, they can be applied in various situations ranging from emergency operations, disaster relief to military service and task forces etc. Obviously, providing security in such scenarios is critical. Several efficient routing protocols have been proposed for Ad-hoc networks. Most of these protocols assume a trusted and cooperative environment. It is crucial to develop efficient routing algorithm with fully protected. In this paper, a new routing algorithm Least Cluster Change(LCC) for ad-hoc network is proposed and implemented to improve the security. That is, trusted network elements that will behave according to the protocol rules. The clusters are formed by excluding the malicious nodes that can be identified by misbehaviour report. The main idea here is to guarantee that all the nodes wishing to participate in the routing process are authenticated nodes Comparing to the contemporary approaches, this proposed routing method demonstrates higher security rates.

To Cite This Article: A. Swaminathan, K. Parkavi, Dr. P. Vivekanandan, S. Arun Rajesh., Secure and Cluster Based Ad-hoc Routing Using Misbehaviour Report Authentication. ***Aust. J. Basic & Appl. Sci.,*** *8(18): 65-71, 2014*

INTRODUCTION

Mobile ad-hoc network consists of nodes that are able to communicate through the use of wireless mediums and form a dynamic topologies. The basic characteristic of these networks is the complete lack of any kind of infrastructure and therefore, the absence of dedicated nodes that provide network management operations do the traditional routers in fixed networks. In order to maintain the connectivity in a mobile ad-hoc network, all the participating nodes have to perform routing of network traffic. The cooperation of nodes cannot be enforced by a centralized administration authority which does not exist. Therefore, a network-layer protocol designed for such self-organized networks must enforce connectivity and security requirements in order to guarantee the undisrupted operation of the higher layer protocols. Unfortunately, all of the widely used ad-hoc routing protocols have no security considerations and trust all the participants to correctly forward routing and data traffic.

The overall design of a solution for all the problems in an ad-hoc network is currently too complex. In this paper, one of these issues, is investigated providing security in an ad-hoc network and it is focused specifically on routing scheme to support security.

Due to the lack of physical protection and reliable medium access mechanism, packet dropping attack represents a serious threat to the routing function in an wireless ad-hoc networks. An intruder can easily join the network and compromise a legitimate node then subsequently start dropping packets that are expected to be relayed in order to disrupt the regular communications. Consequently, all the routes passing through this node fail to establish a correct routing path between the source and destination nodes. Although upper layer acknowledgment, such as TCP-ACK (Transmission Control Protocol ACKnowledgment) can detect end-to-end communication break, it is unable to identify the node which is responsible for communication faults. Moreover, such mechanism is unavailable in connectionless transport layer protocols like UDP (User Datagram Protocol). Therefore, securing the basic operation of the network becomes one of the primary concerns in hostile environments in the presence of packets droppers. The challenge lies in securing communication meanwhile maintaining connectivity between nodes despite of the attacks launched by the foes and the frequently changing topology. It is thus obvious that both phases of the communication, mainly route discovery and data

Corresponding Author: A. Swaminathan, Research scholar, Department of Computer Science and Engineering, CEG, Anna University, Chennai, India.
E-mail: linuxswami@yahoo.com

transmission phase, should be protected, calling for comprehensive security studies (Miranda, H. and L. Rodrigues, 2002).

Additionally, due to the nodes' lack of physical protection, malicious attackers can easily capture and compromise nodes to achieve attacks. In particular, considering the fact that most routing protocols in an ad-hoc environment assume that every node in the network behaves cooperatively with other nodes and presumably not malicious, attackers can easily compromise network operations by inserting malicious or non-cooperative nodes into the network. Furthermore, because of distributed architecture and changing topology, a traditional centralized monitoring technique is no longer feasible in an ad-hoc network.

The use of wireless links makes the networks susceptible to attack. Eavesdroppers can access secret information, violating network confidentiality. Hackers can directly attack the network to delete messages, inject erroneous messages, or impersonate a node, which violates availability, integrity, authentication, and no repudiation. Compromised nodes also can launch attacks from within a network. In the next section, It is mainly concentrated on discussing the background information required for understanding this research topic.

II.Related Work:

The security and the misbehavior problems of wireless networks including ad-hoc networks have been studied by many researchers, e.g., (Zhou, L. and Z.J. Haas, 1999; Stajano, F. and R. Anderson, 1999; Kong, J., 2001; Aad, I., 2004). Various techniques have been proposed to prevent malicious act in ad-hoc Networks.

a) Credit-Based Schemes:

The basic idea of credit-based schemes is to provide incentives for nodes to faithfully perform networking functions. In order to achieve this goal, virtual currency or similar payment system may be set up. Nodes get paid for providing services to other nodes. When they request other nodes to help them for packet forwarding, they use the same payment system to pay for such services (Buttyan, L. and J.P. Hubaux, 2000; Hubaux, J.P., 2001; Jakobsson, M., 2003; Buttyan, L. and J.P. Hubaux, 2003).

Buttyan and Hubaux used the concept of nuggets as payments for packet forwarding in (Buttyan, L. and J.P. Hubaux, 2000). They proposed two models which are the Packet Purse Model and the Packet Trade Model. In the Packet Purse Model, nuggets are loaded into the packet before it is sent. The sender puts a certain number of nuggets on the data packet to be sent. Each intermediate node earns nuggets in return for forwarding the packet. If the packet exhausts its nuggets before reaching its destination, then it is dropped. In the Packet Trade Model, each intermediate node "buys" the packet from the previous node for some nuggets and "sells" it to the next node for more nuggets. Thus, each intermediate node earns some nuggets for providing the forwarding service and the overall cost of sending the packet is borne by the destination.

Each node maintains a counter termed the nugget counter in (Buttyan, L. and J.P. Hubaux, 2003). The counter is decreased when the node sends packets of its own, but increased when it forwards packets for the other nodes. The counter should be positive before a node is allowed to send its packet. Therefore, the nodes are encouraged to continue to help other nodes. Tamper resistant hardware modules are used to keep nodes from increasing the nugget counter illegally.

Another credit-based scheme, termed Sprite, was proposed by Zhong *et al*. (2003). In Sprite, nodes keep receipts of the received/forwarded messages. When they have a fast connection to a Credit Clearance Service (CCS), they report all of these receipts. The CCS then decides the charge and credit for the reporting nodes. In the network architecture of Sprite, the CCS is assumed to be reachable through the use of the Internet, limiting the utility of Sprite. The main problem with credit-based schemes is that they usually require some kind of tamper-resistant hardware and/or extra protection for the virtual currency or the payment system.

b) Reputation-Based Schemes:

The second category of techniques to combat node misbehavior in an ad-hoc network is reputation-based (Marti, S., 2000; Buchegger, S. and J.Y. Le Boudec, 2002). In such schemes, network nodes collectively detect and declare the misbehavior of a suspicious node. Such a declaration is then propagated throughout the network so that the misbehaving node will be cut off from the rest of the network.

In Marti *et al*. (2000) proposed a scheme that contains two major modules, termed watchdog and path rater to detect and mitigate respectively. This is routing misbehavior in ad-hoc. Nodes operate in a promiscuous mode wherein the watchdog module overhears the medium to check whether the next-hop node faithfully forwards the packet. At the same time, it maintains a buffer of recently sent packets. A data packet is cleared from the buffer when the watchdog overhears the same packet being forwarded by the next-hop node over the medium. If a data packet remains in the buffer for too long, the watchdog module accuses the next hop neighbor of misbehaving. Thus, the watchdog enables misbehavior detection at the forwarding level as well as the link level. Based on the watchdog's accusations, the path rater module rates every path in its cache and subsequently chooses the path that best avoids misbehaving nodes. Due to its reliance on overhearing, however, the watchdog technique may

fail to detect misbehavior or raise false alarms in the presence of ambiguous collisions, receiver collisions, and limited transmission power, as explained in (Marti, S., 2000).

The CONFIDANT protocol proposed by Buchegger and Le Boudec in (Buchegger, S. and J.Y. Le Boudec, 2002) is another example of reputation-based schemes. The protocol is based on selective altruism and utilitarianism, thus making misbehavior unattractive. CONFIDANT consists of four important components that are the Monitor, the Reputation System, the Path Manager, and the Trust Manager. They perform the vital functions of neighborhood watching, node rating, path rating, sending and receiving alarm messages, respectively. Each node continuously monitors the behavior of its first-hop neighbors. If a suspicious event is detected, details of the event are passed to the Reputation System. The significant result is obtained from reputation system at different frequent level and it modifies the rating of the suspected node. Once the rating of a node becomes intolerable, control is passed to the Path Manager, which accordingly controls the route cache. Warning messages are propagated to other nodes in the form of an Alarm message sent out by the Trust Manager. The Monitor component in the CONFIDANT scheme observes the next hop neighbor's behavior using the overhearing technique. This causes the scheme to suffer from the same problems as the watchdog scheme.

Miranda and Rodrigues adopted a similar approach in [1]. Each node i maintains a data structure Status i[j] about every other node j as an indication of what impression node i has about node j. Along with a credit counter, node I also maintains lists of nodes to which node j will and will not provide service. Every node periodically broadcasts relevant information in the form of a self-state message. Other nodes update their own lists based on the information contained in these self-state messages.

c) Acknowledgement Schemes:

i) End to end ACK scheme:

In the TCP protocol, end-to-end acknowledgment is employed. Such acknowledgments are sent by the end receiver to notify the sender about the reception of data packets up to some locations of the continuous data stream. The Selective Acknowledgment (SACK) technique is used to acknowledge out-of-order data blocks.

ii) 2ACK scheme:

The 2ACK scheme detects misbehavior through the use of a new type of acknowledgment packet, termed 2ACK. The 2ACK packet is assigned a fixed route of two hops (three nodes) in the opposite direction of the data traffic route.

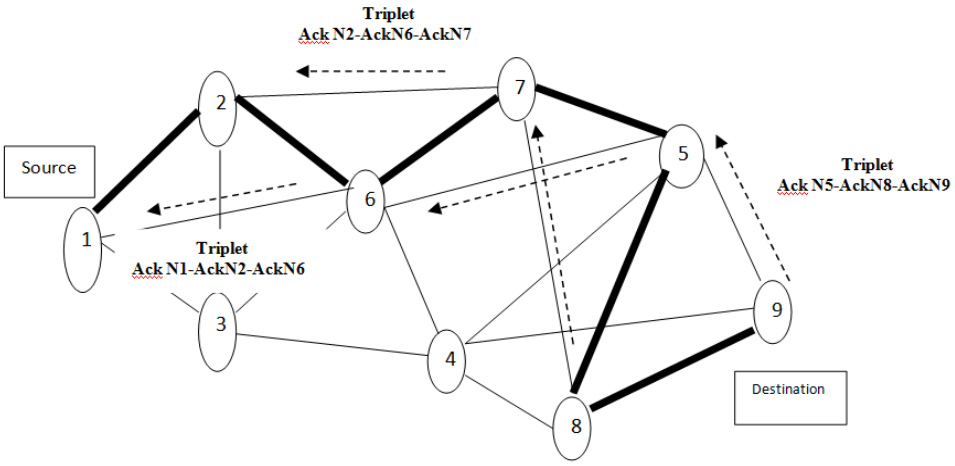

Fig. 1: 2ACK scheme.

Figure.1 illustrates the operation of the 2ACK scheme. Suppose that N1, N2, and N3 are three consecutive nodes (triplet) along a route. The route from a source node S to a destination node D is generated in the Route Discovery phase of the DSR protocol. When N1 sends a data packet to N2 and N2 forwards it to N6, it is unclear to N1 whether N6 receives the data packet successfully or not. Such an ambiguity exists even when there are no misbehaving nodes. The problem becomes much more severe in an open ad-hoc network with potential misbehaving nodes. The 2ACK scheme requires an explicit acknowledgment to be sent by N6 to notify N1 of its successful reception of a data packet.When node N6 receives the data packet successfully, it sends out a 2ACK packet over two hops to N1 (i.e., the opposite direction of the routing path as shown), with the ID of the corresponding data packet. The triplet [AckN1 -AckN2 – AckN6] is derived from the route of the original data traffic. Such a triplet is used by N1 to monitor the link N2 – N6. For convenience of presentation, AckN1 in the triplet [AckN1 -AckN2 – AckN6] is termed as the 2ACK packet receiver or the observing node and AckN6 the 2ACK packet sender.

III.System Description:

The proposed routing protocol consists of five major divisions.

EEACK (End-to-End Acknowledgement), S-ACK (Secure Acknowledgement), Misreporting Authentication, Clustering and Key exchange.

i) EEACK:

The EEACK is suited when no network misbehaviour is detected. In Figure. 2, in EEACK mode, node S first sends out an ACK data packet to the destination node D .If all the intermediate nodes along the route between nodes S and D are cooperative and node D successfully receives packet, and node D is required to send back an acknowledgment packet along the same route but in a reverse order. Within a predefined time period, if node S receives an acknowledgement, then the packet transmission from node S to node D is successful. Otherwise, node S will switch to S-ACK mode by sending out an S-ACK data packet to detect the misbehaving nodes in the route.

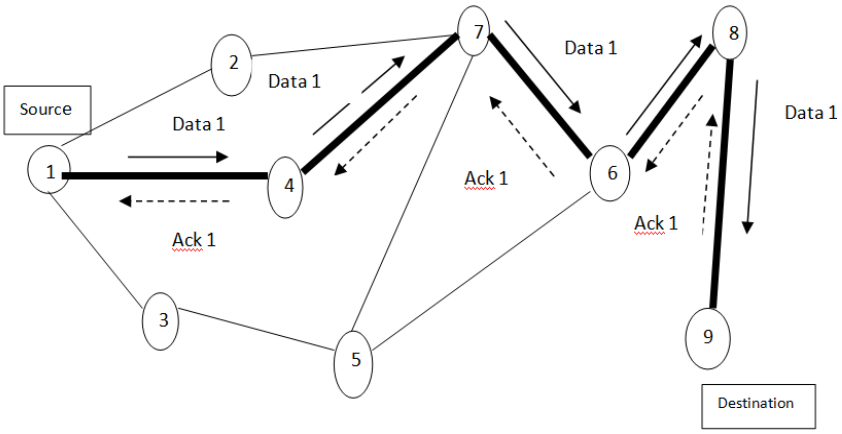

Fig. 2: EEACK scheme.

ii) S-ACK:

The S-ACK scheme is an improved version of the TWOACK scheme proposed by (Kejun Liu *et al.* Kejun Liu, 2007). The principle is to let every three consecutive nodes work in a group to detect misbehaving nodes. For every three consecutive nodes in the route, the third node is required to send an S-ACK acknowledgment packet to the first node. The intention of introducing S-ACK mode is to detect misbehaving nodes in the presence of receiver collision or limited transmission power. As shown in Figure. 2, in S-ACK mode, the three consecutive nodes (i.e., S, A, and B) work in a group to detect misbehaving nodes in the network. Node S first sends out data packet *Spkt*1 to node A. Then, node A forwards this packet to node B. When node B receives *Spkt*1, as it is the third node in this three-node group, node B is required to send back an ACK acknowledgment packet S*ak*1 to node A. Node A forwards S*ak*1 back to node S. If node S does not receive this acknowledgment packet within a predefined time period, both nodes A and B are reported as malicious. Moreover, misbehaviour report will be generated by node F1 and sent to the source node S.

In the 2ACK scheme, the source node immediately trusts the misbehaviour report, But the proposed routing protocol requires the source node to switch to MRA mode and confirm this misbehaviour report. This is a vital step to detect false misreporting about node's behavior.

iii) Misreporting Authentication:

This scheme is designed by Elhadi *et al*., (2013) to resolve the weakness of Watchdog when it fails to detect misbehaving nodes with the presence of false misbehaviour report. The false misbehavior report can be generated by malicious attackers to falsely report innocent nodes as malicious.

This attack can be lethal to the entire network when the attackers break down sufficient nodes and thus cause a network division. The core of MRA scheme is to authenticate whether the destination node has received the reported missing packet through a different route. To initiate the misreporting authentication mode, the source node first searches its local knowledge base and seeks for an alternative route to the destination node. If there is no other that exists, the source node starts a DSR routing request to find another route. Due to the nature of Ad-hoc networks, it is common to find out multiple routes between two nodes. By adopting an alternative route to the destination node, it is circumvent the misbehaviour reporter node. When the destination node receives an authentication packet, it searches its local knowledgebase and compares if the reported packet was received. If it is already received, then it is safe to conclude that this is a false misbehavior report and whoever generated this report is marked as malicious. Otherwise, the misbehaviour report is trusted and accepted.

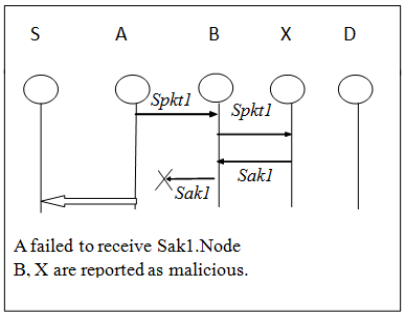

Fig. 3: Proposed Routing Scheme.

iv) Clustering:

By the adoption of misreporting authentication scheme, SAACK is capable of detecting malicious nodes despite the existence of false misbehavior report .The attackers are smart enough to forge acknowledgment packets. In order to ensure the integrity, it requires all acknowledgment packets to be digitally signed before they are sent out and verified until they are accepted. However, the extra resources are required with the introduction of digital signature in MANETs. To address this concern, clustering and key exchange schemes are implemented in the proposed optimal level of security in Ad-hoc environment.

In this step, the clusters are formed among the ad-hoc nodes by excluding the misbehaving nodes. By having a cluster head controlling a group of ad-hoc nodes, a framework for code separation (among clusters), channel access, routing, and bandwidth allocation can be achieved. A cluster head selection algorithm is utilized to elect a node as the cluster head using a distributed algorithm within the cluster. The disadvantage of having a cluster head scheme is that frequent cluster head changes can adversely affect routing protocol performance since nodes are busy in cluster head selection rather than packet relaying. Hence, instead of invoking cluster head reselection every time the cluster membership changes, a Least Cluster Change (LCC) clustering algorithm is introduced. Using LCC, cluster heads only change when two cluster heads come into contact, or when a node moves out of contact of all other cluster heads.

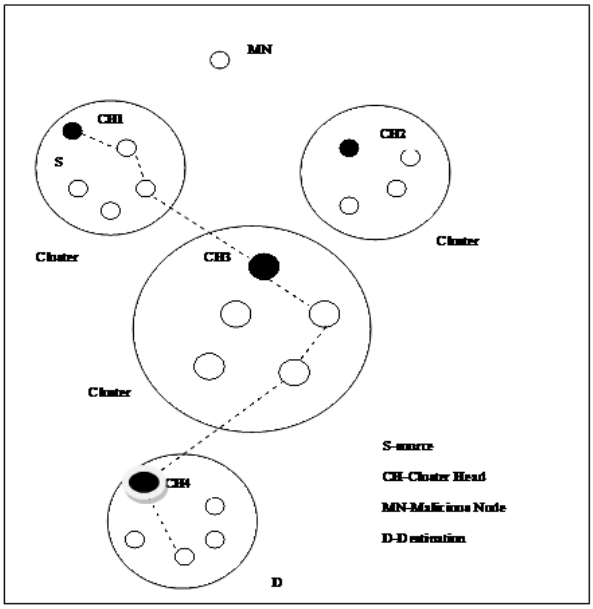

Fig. 4: Clustering scheme.

Using this method, each node must keep a cluster member table where it stores the destination cluster head for each mobile node in the network. These cluster member tables broadcast by each node periodically using the DSDV algorithm. Nodes update their cluster member tables on reception of such a table from a neighbour. In addition to the cluster member table, each node must also maintain a routing table which is used to determine the next hop in order to reach the destination. On receiving a packet, a node will consult its cluster member table and routing table to determine the nearest cluster head along the route to the destination. Next, the node will check its routing table to determine the next hop used to reach the selected cluster head.

v) Key Exchange:

A packet sent by a source node is encrypted with a private key1 and it is first routed to its nearest cluster head. Then the cluster head encrypts the received packet with a key2 and the packet is broadcast to its members. On receiving a packet ,the members decrypt the packet with their group session key .If the key value matches, then it is confirmed the packet is destined to that particular node. Otherwise, the nodes forward the packet to the nearest cluster head. After particular time period, the source node reveals the key1 to the cluster heads. Then the cluster head reveals the key1 if it finds the destination in the cluster. The destination node can decrypt the packet with the key 1.In this method, the two level security are achieved by making the packet first encrypted by the source node and again encrypted by the cluster head.

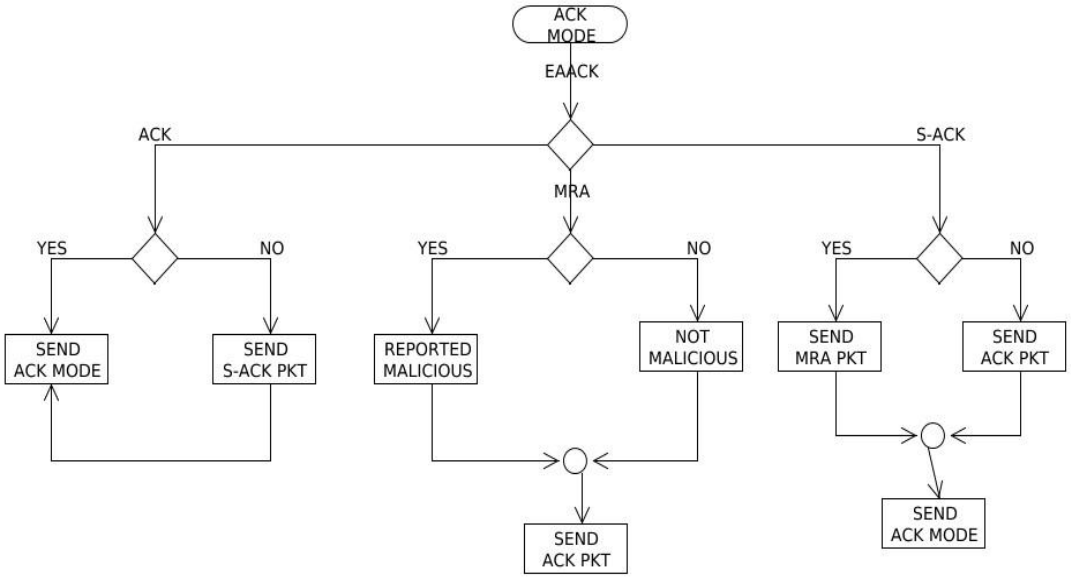

Fig. 5: Flow Diagram for Proposed routing protocol.

IV.Simulation:

The evaluations are performed using the Network Simulator NS-2. The observation period of the proposed routing scheme was set to Tobs =0:20 seconds. The IEEE 802.11 MAC was used with a channel data rate of 11 Mbps. The data packet size was 512 bytes. The wireless transmission range of each node was R =250 m. In the simulations, various numbers of mobile nodes were randomly distributed in a 800 m * 800 m flat area. The source and the destination nodes were randomly chosen among all nodes in the network. The total simulation time was 800 seconds. A random way-point mobility model was assumed with a maximum speed of Vm =30 m/sec. Simulations for constant node speeds of 0, 1, 5 and 10 m/s, with pause time fixed at 30 seconds were run.

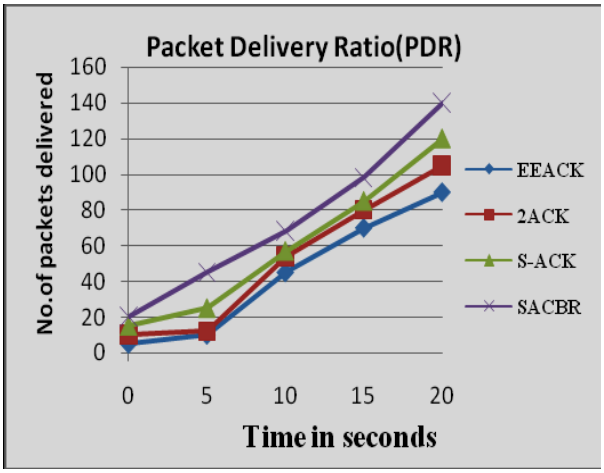

Fig. 6: Packet delivery ratio.

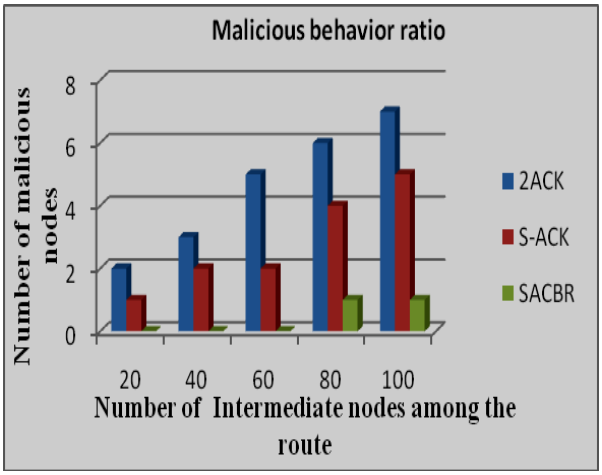

Fig. 7: Malicious nodes ratio.

Table I: Comparision of Simulation Results.

Packet delivery ratio	Malicious 0%	Malicious 10%	Malicious 20%	Malicious 30%	Malicious 40%
ACK	1	0.84	0.6	0.68	0.66
SACK	1	0.86	0.7	0.7	0.91
Secured Cluster Based	1	0.96	0.98	0.92	0.92
Routing overhead	Malicious 0%	Malicious 10%	Malicious 20%	Malicious 30%	Malicious 40%
ACK	0.015	0.025	0.023	0.022	0.023
SACK	0.016	0.035	0.024	0.033	0.025
Secured Cluster Based	0.3	0.3	0.037	0.047	0.61

V.Conclusion:

Wireless communication research primarily focuses on the functional aspect of ad-hoc networks improving the guaranteed delivery of packets from one node to another node . However, as technology matures, nonfunctional properties such as semantics and security will play the leading role. In this proposed method, when the number of node increases ,the amount of encryption level is increased but it finds the malicious nodes perfectly. If ad-hoc communication is to be the foundation for pervasive computing, one must be able to seamlessly interconnect different platforms and devices, offer services on demand, and make it all secure and trusted. In the previous research works, numerous techniques have been proposed in the routing problem in Ad-hoc networks. But the newly proposed method of this acknowledgment and clustered routing decision provides a higher amount of reliability of network.

REFERENCES

Aad, I., J.P. Hubaux and E.W. Knightly, 2004. “Denial of Service Resilience in Ad-Hoc Networks,” Proc. MobiCom.

Buchegger, S. and J.Y. Le Boudec, 2002. “Performance Analysis of the CONFIDANT Protocol: Cooperation of Nodes, Fairness in Dynamic Ad-Hoc Networks,” Proc. MobiHoc.

Buttyan, L. and J.P. Hubaux, 2000. “Enforcing Service Availability in Mobile Ad-Hoc WANs,” Proc. MobiHoc.

Buttyan, L. and J.P. Hubaux, 2003. “Stimulating Cooperation in Self-Organizing Mobile Ad Hoc Networks,” ACM/Kluwer Mobile Networks and Applications, 8(5).

Elhadi M. Shakshuki, Nan Kang and Tarek R. Sheltami, 2013. EAACK-A Secure Intrusion-Detection System for MANETs”, IEEE Trans. on Industrial electronics, 60(3): 1089-1098.

Hubaux, J.P., T. Gross, J.Y. LeBoudec and M. Vetterli, 2001. “Toward Self-Organized Mobile Ad Hoc Networks: The Terminodes Project,” IEEE Comm. Magazine.

Jakobsson, M., J.P. Hubaux and L. Buttyan, 2003. “A Micropayment Scheme Encouraging Collaboration in Multi-Hop Cellular Networks,” Proc. Financial Cryptography Conf.

Kejun Liu, Jing Deng, Pramod K. Varshney and Kashyap Balakrishnan, 2007. ”An Acknowledgment-Based Approach for the Detection of Routing Misbehavior in MANETs, IEEE Trans. on Mobile computing, 6: 536-550.

Kong, J., P. Zerfos, H. Luo, S. Lu and L. Zhang, 2001. “Providing Robust and Ubiquitous Security Support for Mobile Ad-Hoc Networks,” Proc. IEEE Int’l Conf. Network Protocols (ICNP ’01).

Lei Chen and Wendi B. Heinzelman, 2005. QoS-Aware Routing Based on Bandwidth Estimation for Mobile Ad Hoc Networks”, IEEE Journal on Selected areas in communications, 23(3): 561-572.

Marti, S., T. Giuli, K. Lai and M. Baker, 2000. “Mitigating Routing Misbehavior in Mobile Ad Hoc Networks,” Proc. MobiCom.

Miranda, H. and L. Rodrigues, 2002. “Preventing Selfishness in Open Mobile Ad Hoc Networks,” Proc. Seventh Caber Net Radicals Workshop.

Soufiene Djahel, FaridNa¨ıt-abdesselam and Zonghua Zhang, 2011. ”Mitigating Packet Dropping Problem in Mobile Ad Hoc Networks: Proposals and Challenges”, IEEE communications surveys &tutorials, 13(4): 658-679.

Stajano, F. and R. Anderson, 1999. “The Resurrecting Duckling: Security Issues in Ad-Hoc Wireless Networks,” Proc. Seventh Int’l Workshop Security Protocols.

Zhong, S., J. Chen and Y.R. Yang, 2003. “Sprite: A Simple, Cheat-Proof, Credit-Based System for Mobile Ad-Hoc Networks,” Proc.INFOCOM.

Zhou, L. and Z.J. Haas, 1999. “Securing Ad Hoc Networks,” IEEE Network Magazine, 13(6).