ISSN:0975-9646

An Efficient and Secure System for Detecting Malicious Nodes in Mobile Ad hoc Networks

Sruthi. E#, Pradeep. S*

#PG Scholar, *Assistant Professor
Department of CSE, SRM University, Chennai, Tamilnadu, India

***Abstract*— Recent advances in portable computing and wireless technologies are opening up exciting possibilities for the future of wireless mobile networking. A Mobile Ad hoc NETwork (MANET) is one of the most important and unique applications among all the contemporary wireless networks. It consists of mobile platforms which are free to move arbitrarily. They do not need a fixed infrastructure and the network topology may dynamically change in an unpredictable manner. Because of these features it is now popular among critical mission applications like military use or emergency recovery. But security is always an issue for MANET. Due to the node's 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 MANETs assume that every node in the network behaves co-operatively with other nodes and presumably not malicious, attackers can easily compromise MANETs by inserting malicious or non-cooperative nodes into the network. Furthermore, because of MANET's distributed architecture and changing topology, a traditional centralized monitoring technique is no longer feasible in MANETs. In such case, it is crucial to develop an intrusion-detection system (IDS) specially designed for MANETS. Here we proposes a highly efficient and secure IDS by finding out the possibilities of clustering techniques in the existing Enhanced Adaptive ACKnowledgement (EAACK) scheme to further reduce the network overhead and increase the scalability in EAACK system. The main objective of the proposed system is to detect the presence of malicious nodes in the network with less routing overhead and also improving the reliability, throughput and stability of the network efficiently.**

***Keywords*— Clustering, Enhanced Adaptive ACKnowledgement (EAACK), Intrusion Detection system (IDS), Mobile Ad hoc NETwork(MANET), Routing overhead.**

I. INTRODUCTION

Now a days, Mobile ad hoc network (MANET) is one of the recent active fields and has received marvelous attention because of their self configuration and self maintenance capabilities [7]. An ad hoc network is a collection of wireless mobile nodes that forms a temporary network without any centralized administration. In such an environment, it may be necessary for one mobile node to enlist other hosts in forwarding a packet to its destination due to the limited transmission range of wireless network interfaces. Each mobile node operates not only as a host but also as a router forwarding packets for other mobile nodes in the network that may not be within the direct transmission range of each other. Each node participates in an ad hoc routing protocol that allows it to discover multihop paths through the network to any other node. This idea of Mobile ad hoc network is also called infrastructureless networking[14], since the mobile nodes in the network dynamically establish routing among themselves to form their own network on the fly .

While early research effort assumed a friendly and cooperative environment and focused on problems such as wireless channel access and multihop routing, security has become a primary concern in order to provide protected communication between nodes in a potentially hostile environment. Recent wireless research indicates that the wireless MANET presents a larger security problem than conventional wired and wireless networks. Although mobile ad hoc networks have several advantages over the traditional wired networks, on the other side they have a unique set of challenges. Firstly, MANETs face challenges in secure communication. For example the resource constraints on nodes in ad hoc networks limit the cryptographic measures that are used for secure messages. Thus it is susceptible to link attacks ranging from passive eavesdropping to active impersonation, message replay and message distortion. Secondly, mobile nodes without adequate protection are easy to compromise. An attacker can listen, modify and attempt to masquerade all the traffic on the wireless communication channel as one of the legitimate node in the network. Thirdly, static configuration may not be adequate for the dynamically changing topology in terms of security solution. Various attacks like DoS(Denial of Service) can easily be launched and flood the network with spurious routing messages through a malicious node that gives incorrect updating information by pretending to be a legitimate change of routing information[1]. Finally, lack of cooperation and constrained capability is common in wireless MANET which makes anomalies hard to distinguish from normalcy. In general, the wireless MANET is particularly vulnerable due to its fundamental characteristics of open medium, dynamic topology, and absence of central authorities, distribution cooperation and constrained capability [2].

II. SURVEY AND ANALYSIS OF EXISTING IDS IN MANET

As discussed above, due to the limitations of most MANET routing protocols, nodes in MANETs assume that other nodes always cooperate with each other to relay data. This assumption leaves the attackers with the opportunities to achieve significant impact on the network with just one or two compromised nodes. To address this problem, an IDS should be added to enhance the security level of MANETs. If MANET can detect the attackers as soon as they enter the network, we will be able to completely eliminate the potential damages caused by compromised nodes at the first time. IDSs usually act as the second layer in MANETs, and they are a great complement to existing proactive approaches [20]. Anantvalee and Wu [4] presented a very thorough survey on contemporary IDSs in MANETs. In this section, it mainly describe the existing approaches, namely, Watchdog [12], TWOACK [10], Adaptive ACKnowledgment (AACK) [18] and Enhanced Adaptive ACKnowledgement(EAACK)[15].

1) Watchdog: Marti *et al.* [12] proposed a scheme named Watchdog that aims to improve the throughput of network with the presence of malicious nodes. In fact, the Watchdog scheme is consisted of two parts, namely, Watchdog and Pathrater. Watchdog serves as an IDS for MANETs. It is responsible for detecting malicious node misbehaviors in the network. Watchdog detects malicious misbehaviors by promiscuously listening to its next hop's transmission. If a Watchdog node overhears that its next node fails to forward the packet within a certain period of time, it increases its failure counter. Whenever a node's failure counter exceeds a predefined threshold, the Watchdog node reports it as misbehaving. In this case, the Pathrater cooperates with the routing protocols to avoid the reported nodes in future transmission.

Many research studies and implementations have proved that the Watchdog scheme is efficient. Furthermore, compared to some other schemes, Watchdog is capable of detecting malicious nodes rather than links. These advantages have made the Watchdog scheme a popular choice in the field. Many MANET IDSs are either based on or developed as an improvement to the Watchdog scheme [10], [16], [17], [18]. Nevertheless, as pointed out by Marti *et al.* [12], the Watchdog scheme fails to detect malicious misbehaviors with the presence of the following: 1) ambiguous collisions; 2) receiver collisions; 3) limited transmission power; 4) false misbehavior report; 5) collusion; and 6) partial dropping.

2) TWOACK: With respect to the six weaknesses of the Watchdog scheme, many researchers proposed new approaches to solve these issues. TWOACK proposed by Liu *et al.* [4] is one of the most important approaches among them. On the contrary to many other schemes, TWOACK is neither an enhancement nor a Watchdog-based scheme. Aiming to resolve the receiver collision and limited transmission power problems of Watchdog, TWOACK detects misbehaving links by acknowledging every data packet transmitted over every three consecutive nodes along the path from the source to the destination. Upon retrieval of a packet, each node along the route is required to send back an acknowledgment packet to the node that is two hops away from it down the route. TWOACK is required to work on routing protocols such as Dynamic Source Routing (DSR) [9]. The working process of TWOACK is shown in Fig. 1.

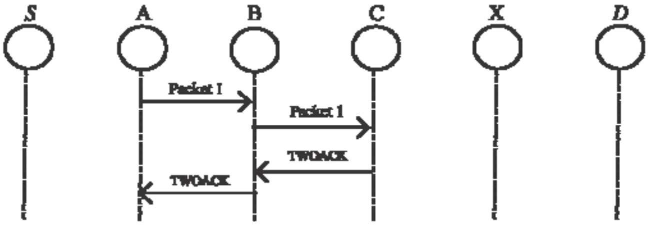

Fig. 1. The TWOACK Scheme

Node A first forwards Packet 1 to node B, and then, node B forwards Packet 1 to node C. When node C receives Packet 1, as it is two hops away from node A, node C is obliged to generate a TWOACK packet, which contains reverse route from node A to node C, and sends it back to node A. The retrieval of this TWOACK packet at node A indicates that the transmission of Packet 1 from node A to node C is successful. Otherwise, if this TWOACK packet is not received in a predefined time period, both nodes B and C are reported malicious. The same process applies to every three consecutive nodes along the rest of the route.

The TWOACK scheme successfully solves the receiver collision and limited transmission power problems posed by Watchdog. However, the acknowledgment process required in every packet transmission process added a significant amount of unwanted network overhead. Due to the limited battery power nature of MANETs, such redundant transmission process can easily degrade the life span of the entire network. However, many research studies are working in energy harvesting to deal with this problem [18], [19], [21].

3) AACK: Based on TWOACK, Sheltami *et al.* [18] proposed a new scheme called AACK. Similar to TWOACK, AACK is an acknowledgment based network layer scheme which can be considered as a combination of a scheme called TACK (identical to TWOACK) and an end-to-end acknowledgment scheme called ACKnowledge (ACK). Compared to TWOACK, AACK significantly reduced network overhead while still capable of maintaining or even surpassing the same network throughput.

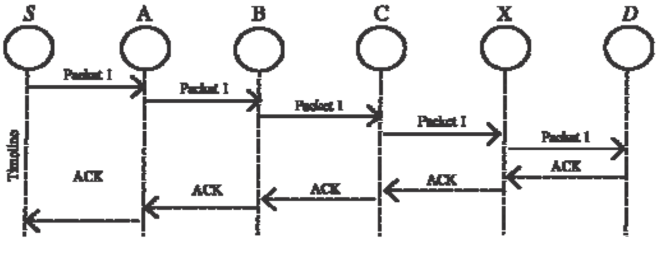

Fig. 2. The ACK Scheme

In the ACK scheme shown in Fig. 2, the source node S sends out Packet 1 without any overhead. All the intermediate nodes simply forward this packet. When the destination node D receives Packet 1, it is required to send back an ACK acknowledgment packet to the source node S along the reverse order of the same route. Within a predefined time period, if the source node S receives this ACK acknowledgment packet, then the packet transmission from node S to node D is successful. Otherwise, the source node S will switch to TACK scheme by sending out a TACK packet. The concept of adopting a hybrid scheme in AACK greatly reduces the network overhead, but both TWOACK and AACK still suffer from the problem that they fail to detect malicious nodes with the presence of false misbehavior report and forged acknowledgment packets. Hence, it is crucial to guarantee that the acknowledgment packets are valid and authentic.

4) EAACK: To mainly address the problem of false misbehavior report and forged acknowledgement packets in TWOACK scheme, Elhadi, Nan Kang and Tarek proposed a scheme named Enhanced AACK (EAACK)[15]. It consisted of three major parts, namely, ACK, secure ACK (S-ACK), and misbehavior report authentication (MRA). ACK scheme acts as a part of the hybrid scheme in EAACK, aiming to reduce network overhead when no network misbehavior is detected. The S-ACK scheme is an improved version of the TWOACK scheme proposed by Liu *et al.* [4]. 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. The MRA scheme is designed to resolve the weakness of Watchdog when it fails to detect misbehaving nodes with the presence of false misbehavior 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.

By the adoption of MRA scheme, EAACK is capable of detecting malicious nodes despite the existence of false misbehavior report. Since it is an acknowledgment based IDS, to ensure that all acknowledgment packets in EAACK are authentic and untainted, all acknowledgment packets are digitally signed before they are sent out and verified until they are accepted.EAACK is required to work on existing flat routing protocols such as Dynamic Source Routing[9]. Though it demonstrates positive performances against Watchdog, TWOACK, and AACK in the cases of receiver collision, limited transmission power, and false misbehavior report it generates more routing overhead in most of the cases.

By maintaining EAACK's ability to improve the network's Packet Delivery Ratio when the attackers are smart enough to forge Acknowledgement packets , we can considerably reduce the network overhead by incorporating the cluster based routing. Clustering not only makes the communication faster, but also it enhances the intrusion detection in the network in such a way that the malicious nodes are detected and isolated as soon as they try to enter the network.

III. Cluster Based Adaptive Acknowledgement Scheme

EAACK scheme surely is an effective IDS that can be used in MANETs. But, network overhead and limited transmission power are still a problem. It is mainly because all the nodes in the networks are equity, and functions as terminal as well router. There is difference in performance instead of function. The main advantage of the MANET structure is that there are multiple paths between source-destination pairs. So it can distribute traffic into multiple paths, decrease congestion and eliminate possible "bottleneck". But MANET with the plane structure will increase routing control overhead; the scalability problem is also likely to happen. As a way to overcome those problems cluster-based semi-centralized approach can be adopted that helps in integration of local intrusion detection in a node or in a cluster with network wide global intrusion detection. An adaptive mobile cluster algorithm can sustains the mobility perfectly and maintains the stability and robustness of network architecture[5][6][3]. The main advantages in bringing clustered routing to the system are:

- Immediate discovery and isolation of malicious nodes in the network by cluster heads.
- Reduces the exchange overhead of control messages and strengthens node management.
- Ease to implement the local synchronization of network
- Provides Quality of Service (QoS) routing
- Support the wireless networks with a large number of nodes

3.1 Overview of Clustering

Clustering has been regularly proposed as a means to improve scalability in MANETs[13]. The basic structure of a cluster is shown in Fig. 3. In clustering procedure, a representative of each sub domain (cluster) is 'elected' as a *cluster head* (CH) and a node which serves as intermediate for inter-cluster communication is called *gateway*. Remaining members are called *ordinary nodes*. The boundaries of a cluster are defined by the transmission area of its CH. With an underlying cluster structure, non-ordinary nodes play the role of dominant forwarding nodes.

In the proposed scheme, an ad hoc network is divided into different clusters using a suitable clustering algorithm [8]. The clustering makes the communication between the nodes in the network more efficient, as each cluster is managed by its cluster-head and inter-cluster communication takes place only through the gateway nodes[13]. The task of cluster management in a cluster is delegated to the cluster-head, which is chosen based on the transmission power periodically. The rotation of cluster management responsibility to different nodes ensures a proper load balancing and fault-tolerance in the system . We propose to delegate the cluster-wide intrusion detection responsibility to the cluster-heads, as apart from their default function of cluster management.

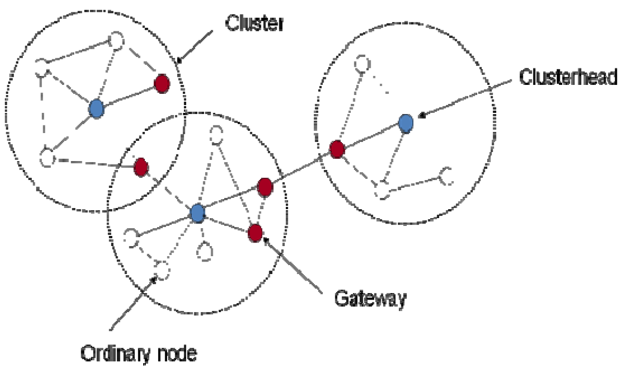

Fig. 3. The Cluster Structure for MANET

Our clustering algorithm considers both location and power information to partition a MANET into separate clusters. Nodes exchange information using the distributed push approach, i.e., every node should broadcast a HELLO message regularly. A cluster member adds its IP address into its HELLO message and a cluster head adds the IP address of its cluster member into its HELLO message as well. To facilitate the cluster head discovery process, cluster member keep the IP addresses of other cluster head that can hear. When the former cluster head moves away or a cluster member does not receive three HELLO packets continuously from its cluster head, it considers that the wireless link between them is broken (or the cluster head has moved away). Thus, a cluster member chooses the latest refresh cluster head in its routing table as its new cluster head, which is one hop from it, or becomes itself a cluster head if it cannot hear any existing cluster head. After broadcasting its HELLO right next packet, the selected cluster head is informed that a new cluster member has joined its group. The cluster member will obtain the confirmation of its new cluster head when it receives the HELLO packet that carries its IP address.

3.2 Cluster Head Updating and Dynamic Route Repairing

When a cluster member node does not receive three HELLO packets continuously from its cluster head, it considers that the wireless link between them is broken. Thus, it must find a new cluster head, which is one hop from it, or becomes itself a cluster head if it cannot hear any existing cluster head. If the route used to forward packets is broken due to node mobility or some link can't meet the QoS requirement, the node deletes the entry of this link from its routing table and selects another redundant labeled links that meet the requirement to forward information. The session traffic, QoS requirement and the link label of the link are switched to the new link. When a new node joins a cluster, the cluster head informs the upward cluster head the IP address of the new member. It sets up multiple disjoint links passing by the new node from the upstream cluster members to the downstream cluster members. When some link breaks or can't satisfy the requirement, it chooses one of the new links across the new node to replace the old link, and then, switches the session traffic, QoS requirement and the link label of the link to the new link.

3.3 Route discovery

A computer network is modeled as a graph G=(V,E),where V is set of nodes and E is set of edges(links).Let S be the source node and D be the destination node. A cluster is denoted by Ci={N_{ij}},where N_{ij} is the member of cluster i. Let CHi be the cluster head of C_i. It is defined the successor set of node N_{ij} in cluster Ci as S_{ij} and the predecessor set as D_{ij}. When a source node S (S ∈ C_1) seeks to set up a connection to a destination D, S sends a route request message(RREQ) to its cluster head CH_1.The RREQ message includes the fields as shown in Fig.4.

If D is a member of cluster C_1 as well and hears the request message, then

1. it sets up multiple paths from source node S to next hop nodes $D(N_{ij})=\{C_i-N_{ij} , i=1,N_{ij}=S\}$;
2. then sets up multiple path from the source nodes $S(N_{ij})=\{C_i-N_{ij},i=1,N_{ij}=D\}$ to destination node D.
3. it selects all the reliable link disjoint paths from S to D($P \geq P_{lower}$, where P is reliability and P_{lower} is lowest reliability).
4. if all paths have been established, then it chooses the maximal disjoint and loop-freedom reliable paths that satisfies above conditions.

Source Address S
Destination Address D
Session ID
Plower
QoS request
Virtual Route VR

Fig. 4. RREQ message

If destination node D is not in the same cluster as source node S, then

1. source node S sends a route request message(RREQ) to its cluster head CH_1. CH_1 looks for which cluster the destination node D belongs to, then searches for a stable route as a directional guideline {S , C_2 , … , C_{m-1} , D }.At the same time, it sets up multiple links from source node S to the destination nodes set $D(N_{ij})=\{C_i-S , i=1\}$, nodes set $D(N_{ij})=\{C_i-\sum N_{ij}$, $\sum N_{ij}$ denoted as nodes set between source node S and N_{ij} , i=1} as next hop address, the hop of the links is likely more than one.
2. cluster head CH_1 sends the RREQ message to its downstream cluster C_2. Once CH_2 receives this message, it will send the RREQ to next cluster and report the IP addresses of its cluster members to CH_1 at one time.
3. then, it sets up disjoint links: $\{N_{1j} \rightarrow N_{2j}\}$, ($N_{1j} \in C_1$, $N_{2j} \in C_2$);
4. C_{i-1} passes the RREQ messages to C_i. Once CH1 receives the message, CH_i reports the addresses of its cluster members to $C_{i-1,}$ and passes the RREQ to C_{i+1}; 5).

5. then, it sets up multiple disjoint links: $\{N_{i-1j} \rightarrow N_{ij}\}$, ($N_{i-1j} \in C_{i-1}$, $N_{ij} \in C_i$);
6. It sets up links from the members of C_i Si={ N_{ij} }(as source nodes) to the members of cluster Ci except the N_{ij} $\{C_i\text{-}N_{ij}\}$ (as destination nodes), $\{C_i\text{-}\sum N_{ij\ -1}\}$ as next hop addresses, and chooses the links that satisfies the reliability request ($P \geq P_{lower}$), the hop of the links is likely more than one ;
7. When the cluster head CH_m where the destination locates recieves the path request message, cluster Cm will set up disjoint multiple links from S_m={ C_i-D } (as source nodes) , $D(N_{ij})=\{C_i\text{-}\sum N_{ij\ -1}\}$ as next hop address, to destination node D, and choose the links that satisfies the reliability request ($P \geq P_{lower}$) ;
8. Finally, when all complete paths to destination node have been established, it will choose all maximal disjoint, loop-freedom reliable paths that satisfy above conditions based on hop number and bandwidth.

The above paths just are possible routes called as virtual routes.

The reverse link labeling algorithm tries to find as many as possible real routes that are along the virtual path with loop-freedom and satisfy the QoS requirement for this particular session as well. The destination D generates a one-hop broadcast, sending the reverse labeling message called RREP. The reverse labeling message includes the fields as shown in Fig.5:

Source Address S
Labeling Source Address L
Session ID
Plower
QoS request
Virtual Route VR
Hop H
Accumulated Delay AD

Fig. 5. RREP message

Before starting the reverse-link labeling phase, D sets L as its IP address, H as 0 and AD as 0 while other fields are the same with those in the route request message. Every node that receives the reverse labeling message checks whether it meets the following conditions in order to broadcast the packet again after:

- increasing H by 1;
- adding its delay to AD;
- recording L, H and AD into its routing table;
- replacing L with its IP address, L must meet the following requirement:
  a) It belongs to a cluster head that is in the virtual route VR.
  b) It has enough bandwidth.
  c) The accumulated delay AD does not exceed the delay requirement in QoS.
  d) The hop number H does not exceed the maximum hop (H_{max}).
  e) It is neither a leaf node nor the source node S.
  f) The intermediate nodes also record the labeling information from other labeling source address L with a bigger H (not 2 hops bigger than the maximum hop number) but do not broadcast it.

Thus, more than one route will be discovered between S and D that comprise of links labeled by session ID.

3.4 Malicious Node Detection

According to the cluster Based Multipath Routing, the source node sets up multiple paths from source node to destination node based on the hop number (h), accumulated delay (AD) and bandwidth(b) included in the paths messages received by source. The data packet is then fragmented into smaller blocks. These fragments then must be reassembled at the destination node, it maybe lead to error and increase control overhead. So as to avoid it, in our algorithm, the source node decides the best path among multiple routes it have discovered considering the hop number, accumulated delay, bandwidth and available power. Then sends the data packet as in the Enhanced Adaptive Acknowledgement Scheme[15]. We can impose the 3 schemes namely ACK, S-ACK and MRA with less routing overhead.

1) ACK: If no network misbehavior is detected ,ACK part of this hybrid scheme further reduce the overhead in the network with faster and reliable communication. 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.

2) S-ACK: The S-ACK scheme is an improved version of the TWOACK scheme proposed by Liu *et al.* [4]. 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. If the first node does not receive this acknowledgment packet within a predefined time period, both nodes 2 and 3 are reported as malicious. Moreover, a misbehavior report will be generated by node 1 and sent to the source node S. Nevertheless, unlike the TWOACK scheme, where the source node immediately trusts the misbehavior report, EAACK requires the source node to switch to MRA mode and confirm this misbehavior report.

3) MRA: The MRA scheme is designed to resolve the weakness of Watchdog when it fails to detect misbehaving nodes with the presence of false misbehavior 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 MRA 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 routing request to find another route. By adopting an alternative route to the destination node, we circumvent the misbehavior reporter node. When the destination node receives an MRA packet, it searches its local knowledge base 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 misbehavior report is trusted and accepted.

IV. CONCLUSIONS

Security being always a potential issue in MANETs, a system which provides high throughput and packet delivery in a secured manner is designed. In the proposed system, the malicious attacks are efficiently detected with reduced routing overhead than in the existing similar IDS. Since the transmission power and average delay of each node is considered periodically for rout discovery, it avoids the chances to cut the network and assures faster packet transmission. As well, the nodes are given a shared responsibility which makes the network more stable and scalable.

The proposed system focus mainly on packet dropping attack which turns out to be Denial of Service Attacks. In the future we plan to identify different attacks that can be launched in MANETs and will try to bring up more security against those attacks.

REFERENCES

[1] R. H. Akbani, S. Patel, and D. C. Jinwala, “DoS attacks in mobile ad hoc networks: A survey,” in *Proc. 2nd Int. Meeting ACCT* , Rohtak, Haryana, India, 2012, pp. 535–541.

[2] R. Akbani, T. Korkmaz, and G. V. S. Raju, “Mobile Ad hoc Network Security,” in *Lecture Notes in Electrical Engineering*, vol. 127. New York: Springer-Verlag, 2012, pp. 659–666.

[3] A. Alwan, R. Bagrodia, N. Bambos et al.,“Adaptive mobile multimedia networks,” *IEEE Personal Commun*., Apr. 1996, pp. 34-51.

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

[5] A. Bhatnagar and T. G. Robertazzi, “Layer Net: a new self-organizing network protocols,” *Proc. IEEE MILCOM ’90*, pp. 845-849.

[6] M. Gerla and T. C. Tsai, “Multicluster, mobile, multimedia radio network,” *ACM-Baltzer J. Wireless Networks*, vol. 1, no. 3, 1995,pp.255-65.

[7] Himani, Prof.Harwant Singh Arri, “An Efficient Data Sending Under Hybrid Protocol”, *International Journal of Computer Science and Management Research*, Vol 2, Issue 3, March 2013

[8] A.Huiyao, P. Wei and L. Xicheng, “A Cluster-Based Multipath Routing for MANET*”, in part by 973 national momentous foundation research task and national natural science fund(90204005)*.

[9] D. Johnson and D. Maltz, “Dynamic Source Routing in *ad hoc* wireless networks,” in *Mobile Computing*. Norwell, MA: Kluwer, 1996, ch. 5, pp. 153–181.

[10] J.-S. Lee, “A Petri net design of command filters for semiautonomous mobile sensor networks,” *IEEE Trans. Ind. Electron.*, vol. 55, no. 4, pp. 1835–1841, Apr. 2008.

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

[13] A.B. McDonald and T. F. Znati, “A mobilitybased framework for adaptive clustering in wireless ad hoc networks,” *IEEE J. Select. Areas Commun*., vol. 17, no. 8, Aug. 1999, pp. 1466-1487.

[14] National Science Foundation. Research priorities in wireless and mobile communications and networking: Report of a workshop held March 24–26, 1997, Airlie House, Virginia. Available at http://www.cise.nsf.gov/anir/ww.html.

[15] N. Kang, E. Shakshuki, and T. Sheltami, “EAACK- A Secure Intrusion Detection System for MANETs,” *IEEE Trans. Ind. Electron.*, vol. 60, no. 3, March 2013

[16] 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., Commun.*, 2004, pp. 747–752.

[17] A. Patcha and A. Mishra, “Collaborative security architecture for black hole attack prevention in mobile ad hoc networks,” in *Proc. Radio Wireless Conf.*, 2003, pp. 75–78.

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

[19] K. Stanoevska-Slabeva and M. Heitmann, “Impact of mobile ad-hoc net- works on the mobile value system,” in *Proc. 2nd Conf. m-Bus.*, Vienna, Austria, Jun. 2003.

[20] B. Sun, “Intrusion detection in mobile ad hoc networks,” Ph.D. dissertation, Texas A&M Univ., College Station, TX, 2004.

[21] A. Tabesh and L. G. Frechette, “A low-power stand-alone adaptive circuit for harvesting energy from a piezoelectric micropower generator,” *IEEE Trans. Ind. Electron.*, vol. 57, no. 3, pp. 840–849, Mar. 2010.