International Journal of Applied Engineering Research ISSN 0973-4562 Volume 13, Number 23 (2018) pp. 16312-16317
© Research India Publications. http://www.ripublication.com

Using Dynamic Watchdog Optimization Technique for Secure Data Transfer in MANET

Mrs. C. Gayathri
Research scholar,
Department of Information Technology,
School of Computer Science and Engineering
Bharathiar University, Coimbatore, TN – India.

Dr. R. Vadivel
Assistant professor
Department of Information Technology
School of computer science and engineering
Bharathiar University, Coimbatore, TN- India.

Abstract

Energy efficiency and security plays a major role in MANET. To make this possible we are using Dynamic watchdog optimizing technique in two levels. First level of optimization is watchdog location optimizing. This level of optimizing technique use distance based probabilistic algorithm. This algorithm can find a set of watchdog nodes by considering those nodes locations in a probabilistic manner and to create shortest path between source node and destination node. Second level of optimization is uses Dynamic watchdog optimizing. This mechanism play role on as normal node acts as a watchdog node on responsible path. If packets successfully reach the destination a Watchdog node changes into normal node this mechanism called as Dynamic Watchdog Technique. Used for detect malicious node. It defines the number of task to be performed by watchdog node within a time window.

Keywords: MANET, Data transfer, Dynamic Watchdog and Security.

INTRODUCTION

MANET is an infrastructure less network consists of self configuring mobile devices which can move independently in any direction and leads to frequent modification in the transmission links with respect to other devices. One of the limitations in MANET is malicious nodes present in the network. Such nodes can easily corrupt the data in the routing path and finally resulted in malfunctioning of the network operations. Some of the malicious attacks launched in the network corrupted the information that is transmitted among nodes while other attacks might attempt to change the path that they are transmitted to prevent valid node to receive the correct packets [1].

So, security is considered as an important concern in network topology, routing, and data traffic. Many research works have focused on the security of MANETs.

Certificate management mechanism is developed in which trust values are used for providing protected services in the network and applications of network. Components like Prevention, Detection, and revocation are the security solutions utilized for certificate management.

The task of adding and removing the certificates of attacks launching nodes is called certification revocation scheme. This revocation scheme has performed under voting based and non-voting based mechanism.

In voting mechanism, certificate of attacker nodes was revoked based on the votes given by its non attacker neighboring nodes and the latter mechanism consider a given node as malicious attacker with a help of any other node having valid certificate. Thus the certificate of malicious nodes was detected and malicious nodes were removed from the network.

But security during multiparty transmission was not considered by this certificate revocation scheme. According to the behaviour of nodes in MANET systems, the nodes are classified into two types: normal and malicious nodes. A normal node is deemed to secure communications with other nodes.

This node can correctly detect attacks from malicious nodes, accuse them positively, and revoke their certificates in order to guarantee system security [2]. A malicious node does not follow the expected behavior. This node may try to launch several types of attacks; most of these attacks are accomplished by modifying a message before forwarding or simply not forwarding a message that it is supposed to forward. Therefore, the certificates of malicious nodes should be revoked and these nodes should be evicted from the MANET system to maximize the network performance.

A MANET comprises battery powered sensor nodes with extremely restricted processing capabilities. With a narrow radio communication range, a sensor node wirelessly sends messages to a base station via a multi-hop path. However, the multi-hop routing of MANETs often becomes the goal of malicious attacks. An attacker can tamper nodes physically, make traffic collision with seemingly legal transmission, drop or misdirect messages in routes, or jam the communication channel by creating radio interference [3].

A critical complement to security mechanisms trusts systems are widely applied to protect MANET,s from being attacked by trust sensor node. Those nodes can bypass traditional security protections using their trust identities, but can be possibly captured by trust systems due to their poor reputation or past misbehavior. Building trust system is not easy task. The problems which are found while building these trust system are. First, sensor nodes may not be located in the communication range for base station or cluster head. Second, some sensor node may not be communicating with other nodes or it may be communicating with low frequency.

Third, the information obtained from one sensor node cannot be used to build trust system for other sensor nodes. Although the watchdog technique has been proved as a very effective approach to build up MANET Trust System foundations, it introduces a large amount of additional energy consumptions which conflict the energy efficient design principle of MANETs. Recharging or replacement of these MANET nodes‟ power is very difficult and expensive [4, 5].

Due to those challenges, energy saving plays a very important role in the design of modern MANETs. However, to our best knowledge, no existing MANET Trust Systems give appropriate solutions to save the energy consumed by the watchdog technique. In particular, some MANET Trust Systems do not discuss how to schedule watchdogs in their proposals, while some others implicitly suggest letting sensor nodes launch neighbor flooding watchdog tasks to monitor all their neighbors and do not study which frequency is appropriate for their monitoring.

LITERATURE REVIEW

From this section we have reviewed and evaluated the security and privacy problem of existing research works and analyze the drawbacks of the many articles.

N. Aravinthan et al [6] The Mobile Adhoc Network consists of deployed mobile nodes which lead to the frequent changes in network topology. Due to topology changes, required infrastructure is unavailable for communication. Moreover, malicious nodes present in MANET make use of this alteration and can simply launch highly vulnerable attacks on the routing path of the network. Hence, Security concern such as removing misbehaving nodes is the primary issue in MANET. Effective certificate revocation scheme was introduced to identify and remove the node with malicious behavior in the network based on the weighted voting game (ECR-WVG) approach. In this approach, weights and quota were two factors, determined for an effective revocation of malicious nodes certificates. In Effective Certificate Revocation Scheme based on Weighted Voting Game and Rational Secure Multi-Party Computing (ECR-WVG-RSMPC) method, rational secret sharing scheme is introduced along with ECRWVG approach for securing multiparty communication. Performance evaluation can be finished between ECR-WVG and ECR-WVG-RSMPC in terms of false revocation, malicious node revocation, normalized time for revocation and revocation accuracy ratio.

Waleed S. Alnumay and Uttam Ghosh [7] analyze the popular MANET routing protocol AODV and the standard TCP has been improved and made suitable for using it in mobile ad hoc networks. The proposed routing protocol provides security to the route discovery and route maintenance phases. Further, the three-way handshaking process of standard TCP has been secured. Here each node is made to have an ID that is generated from its public key and is unchangeable throughout the lifetime of the network. Performance analysis shows that our proposed protocols are secure against the attacks that are associated with AODV and TCP in MANET

Kartik Kumar Srivastava [8], analyze the information exchange in a network of mobile and wireless nodes without any infrastructure support such networks are called as adhoc networks. A Mobile adhoc network (MANET) is mobile, multi-hop, infrastructure less wireless network which is capable of autonomous operation. In this paper we have discussed some of the basic routing protocols in MANET like Destination Sequenced Distance Vector(DSDV), Dynamic Source Routing(DSR), Ad-hoc On Demand Distance Vector(AODV) and Zone Routing Protocol(ZRP). Security is one of the biggest issue in MANETs as they are infrastructure-less and autonomous. Therefore, in manet networks with security needs, there must be two considerations kept in mind: one to make the routing protocol secure and second one to protect the data transmission. Our endeavor in this paper would focus on achieving the routing and secure information exchange. This will facilitate the user nodes to perform routing, mutual authentications, generation and secure exchange of session key.

Jie Wu, et al. [9], study the privacy threat in multihop wireless networks, with this threat where attacks such as traffic analysis and flow tracing can be simply happened by a malicious challenger due to the Public atmosphere of the wireless medium. For this network coding has the latent one to prevent these attacks since the coding/mixing process is confident at intermediate nodes. However, with the simple exploitation of network coding cannot complete the goal once sufficient packets are composed by the challenger. In other way, with the help of existing privacy-preserving techniques of onion routing, the coding/mixing nature prevents the possibility of exploiting. For this the authors propose network coding based privacy-preserving method beside the traffic analysis in multihop wireless networks [10]. They use the homomorphic encryption mechanism on the Global Encoding Vectors (GEVs), their scheme provides two major privacy-preserving features, packet flow untraceability and message content confidentiality, for competently preventing the traffic analysis attacks. Furthermore, the proposed method keeps the random coding feature, and each sink can make progress the source packets by inverting the GEVs with a very high likelihood.

Yan Sun [11] et al approaches is based on offering members of the location information group keys (GKs) that allows them to decrypt the location information. For this GK management this paper proposes a Rebalancing algorithm to preserve rekeying performance with GK management. This article carries the free coupling throughout a network, thus allows third-party control. This paper provides a protocol like suitable key distribution, Multimedia Internet Keying (MIKEY), and Logical Key Hierarchy (LKH) protocol. These protocols are used to preserve hierarchical location information distribution for supple location privacy control for effectual message delivery and group management complexity [12]. Hence it does not support the multicast communication. And they were computational cost is also high. They were user anonymity problem from this approach.

PROBLEM DEFINITION

It increases energy consumption in MANET. Sensor nodes are usually equipped with limited battery and work in an unattended mode for a long period of time. Rechargement or Replacement of those nodes power is very difficult and expensive. In Existing, system not gives correct solutions to save the energy consumption. Sensor nodes are usually equipped with limited battery, and work in an unattended mode for a long period of time to adapt various harsh environments such as the deep desert and ocean abyss. Due to those challenges, energy saving plays a very important role in the design of modern MANET [12].

However, to our best knowledge, no existing MANET give appropriate solutions to save the energy consumed by the watchdog technique (i.e., the trust-energy conflict induced by watchdog usage has not been addressed before). In particular, some WSNTSs do not discuss how to schedule watchdogs in their proposals, while some others implicitly suggest letting sensor nodes launch neighbour-flooding watchdog tasks to monitor all their neighbors and do not study which frequency is appropriate for their monitoring. This technique is not efficiently identified and blocks the attacking nodes. Decrease the network lifetime.

PROPOSED SYSTEM

However, to our best knowledge, no existing MANET gives appropriate solutions to save the energy consumed by the watchdog technique. The proposed system uses the dynamic optimizing watchdog techniques for MANET. This technique is used to balance energy efficiency and security in terms of trust accuracy and robustness. In this dynamic watchdog optimization method the information sends from source node to destination in the path many of the nodes are available. The neighbour or nearest node will be changed the watchdog for the purpose of reduce the energy consumption. This watchdog is called as a dynamic watchdog. Ultimate goal is to reduce the energy cost induced by watchdog tasks as greatly as possible, while keeping trust accuracy and robustness in a sufficient level.

Watchdog Optimization

To touch this goal using watchdog optimizes techniques in two levels. In first level, to optimize the watchdog locations by giving a target node to minimize overall risk in terms of both energy consumption and security. Watchdog Location Optimization technique using DBP (Distance Based Probabilistic) algorithm to identify the target node and create shortest distance communication. It identifying misbehaving sensor nodes and preventing those nodes from being used for future routing.

So the proposed method concern with energy efficient secure routing algorithm to choose efficient and trustworthy next-hop node in a router. In second level, it optimizes watchdog frequency and reduces its redundancy. By using the Dynamic Watchdog Optimization Algorithm (DWOA) to estimate energy units for each node and detect the malicious node. Based on this energy consumption node it transfers the data to intermediate nodes.

Algorithm: DWOA

The steps of the algorithm as follow:

Step 1: Sender sends the data packets from Source to Destination.

Step 2: The Source find the shortest path and then informed to Cluster Head (CH).

Step 3: The CH is responsible to inform the request response path to the Mobile Sink.

Step 4: Mobile Sink set Dynamic watchdog node on Current path.

Step 5: Dynamic Watchdog Mechanism is done by KP-ABE (Key Policy Attribute Based Encryption) and its energy level is maintained by the corresponding node.

Step 6: If any malicious node occurs the particular path will be discarded by Dynamic Watchdog Node.

Step 7: If malicious node does not occur then the packets are successfully send to their Destination.

Step 8: Finally the Dynamic Watchdog node automatically change into normal node

Pseudo code for Dynamic Watchdog optimization Technique

```
Watchdog( )
Begin
    if  Sender / Forwarder overhears a data packet
begin
    if expected packets
begin
    rewarded as a forwarded packet
    status(nexthop)==good
end
    if sent packets Timeout
begin
   if count(non-forwarded packet) > Threshold
begin
   if status (nexthop) !=good
begin
   send alarm packet to
   source status(nexthop)=malicious
end
end
end
end
end
```

Neighbouring Multi hop routing algorithm

This technique is used to dynamically create shortest path between intermediate nodes to target node. Using the Watchdog Location Optimization techniques to identify the nodes location and using the DBP algorithm to find the minimum location distance of the target node.

Peer Connection

Here the routing is based on Neighboring Multi hop Routing algorithm between nodes. This algorithm is used to calculate the routing path. All the active nodes in WSN, Once the correct destination router is found, an end-to-end peer connection (TCP or IP) is established to carry end-system. This connection remains active as long as the file requested transferred and it is dynamically shut down when not in use [14].

Here the mobile sink node temporarily assigns watch dog for every data transfer, this will avoid delay and waiting time. The allocation of watch dog entirely depends on the distance between the source and destination nodes. Once the node will be assigned as watch dog node, the node will protect the packets from unauthorized access until the process get over. After the successful packet transfer the watch dog node will become normal node.

EXPERIMENTAL RESULT

Simulation Configuration

The Simulation is carried out using the tool Network simulator 2 (NS-2).

S.NO	Parameter	Value
1	Simulator	NS-2
2	Channel Type	Wireless channel
3	Routing protocol	AODV
4	Type of Traffic	CBR
5	MAC Layer	802_11
6	Grid size	500*500
7	No.of.Nodes	100 nodes

Performance Metrics

This Research uses the below metrics to evaluate the proposed algorithm.

- Throughput

$$\frac{\text{No.of data packets sent}}{\text{No.of data packets received}}$$

- Packet Delivery Ratio

$$\frac{\text{Total No.of packets received}}{\text{Total No.of packets Send}}$$

- Packet Loss

  Total number of packet send – total number of packet received

- Routing Overhead

  Total number of routing packets counted once per Hop.

RESULT & DISCUSSION

In this section, the effectiveness of the proposed Dynamic Watchdog Optimization scheme is validated through simulation. Based on the energy consumption node it transfers the data to intermediate nodes. It defines the number of task to be performed by watchdog node within a time window. Below results shows the flow of data transaction from source node to destination node using Dynamic watchdog optimizing technique for selecting the shortest path. It provides lot of advantages like it reduce energy consumption by the sensor nodes by optimizing watchdog in location and frequency.

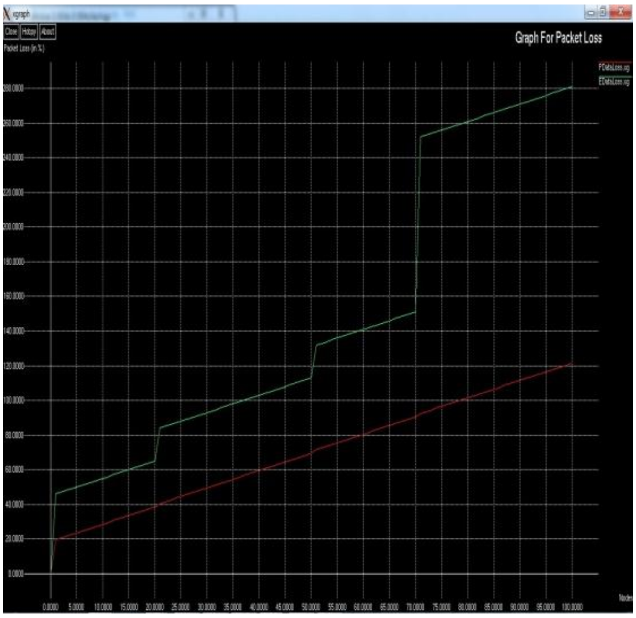


Fig 5.1 Percentage of total packets dropped that passed through the malicious nodes

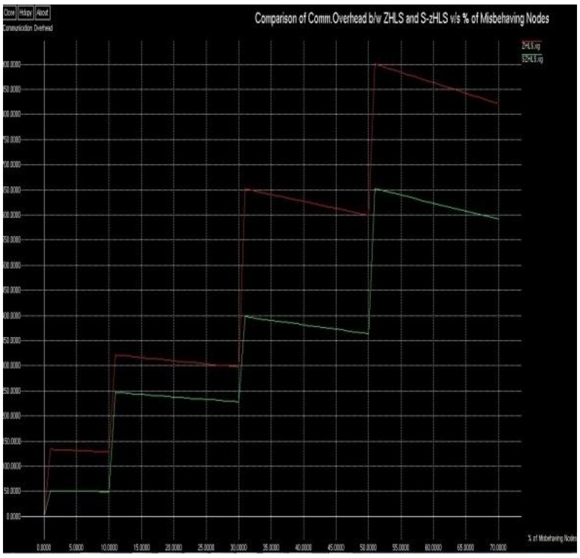
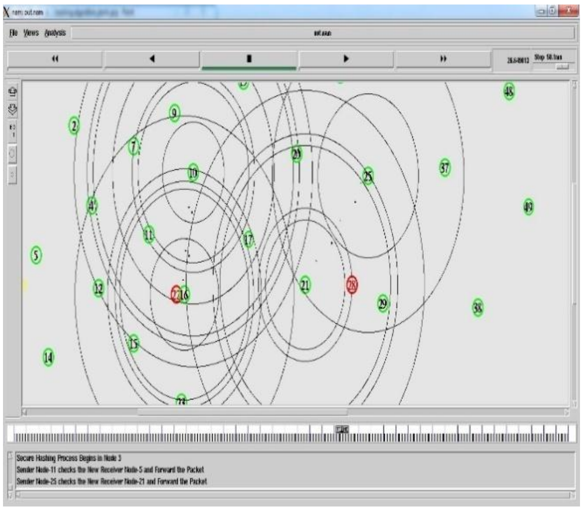


Fig 5.2 Communication Overhead in network construction for Node 100



Secure Hashing Process Begins in Node 3
Sender Node-11 checks the New Receiver Node-5 and Forward the Packet
Sender Node-25 checks the New Receiver Node-21 and Forward the Packet

Fig 5.3 Apply Dynamic watchdog mechanism detect in Malicious Node

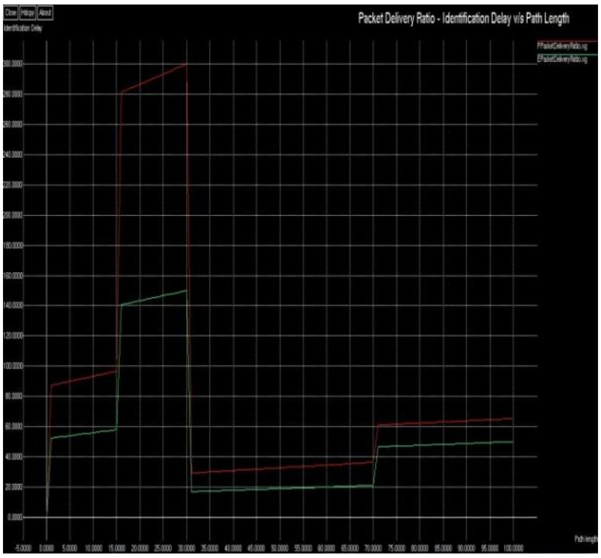


Fig 5.4 Packet Delivery Ratio

It is defined as the segmentation of the data packets produced by the CBR sources that are provided to the destination.

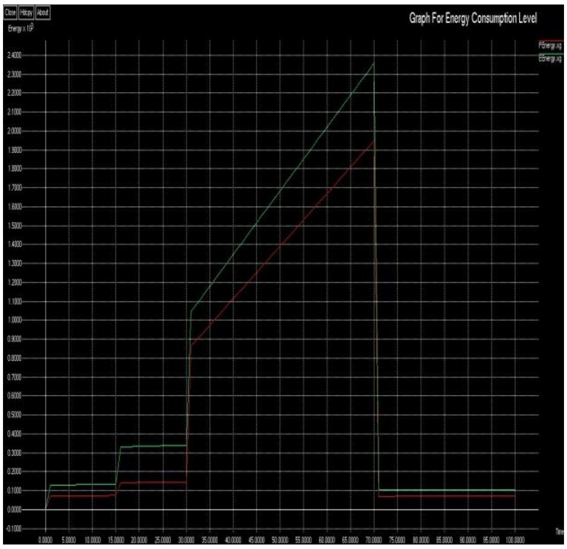
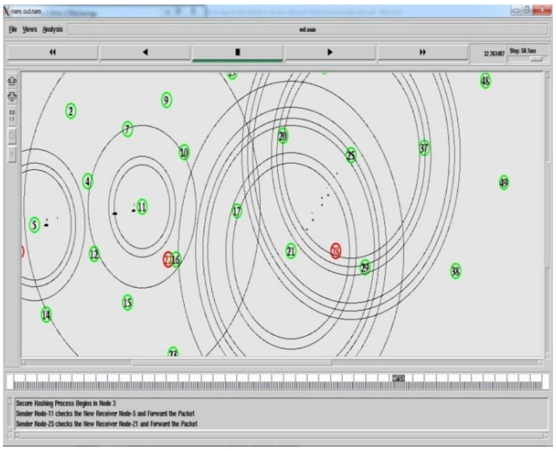


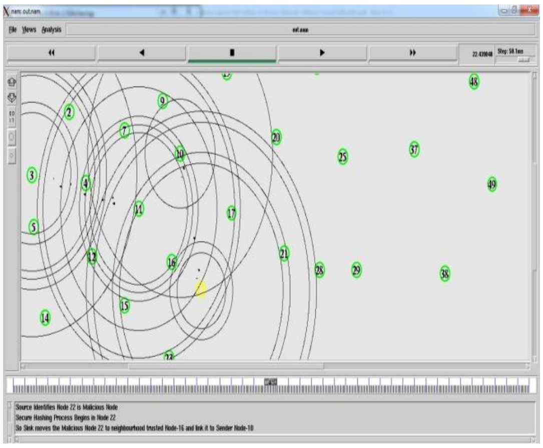
Fig 5.5 Energy Consumption Ratio

The graph shows that for both schemes the communication overhead maintained smoothly and for SHA-ZHLS using SHA it gives the less amount of communication overhead in terms of packet loss ratio at malicious nodes even for 100 nodes.



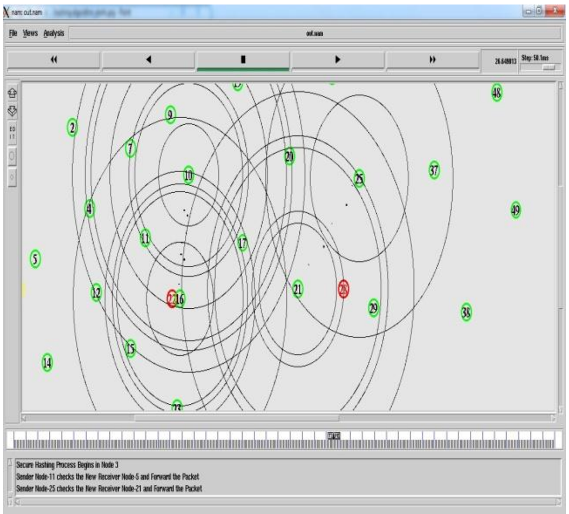
Secure Hashing Process Begins in Node 3
Sender Node-11 checks the New Receiver Node-5 and Forward the Packet
Sender Node-25 checks the New Receiver Node-21 and Forward the Packet

Fig 5.6 Check the new receiver



Source Identifies Node 22 is Malicious Node
Secure Hashing Process Begins in Node 22
So Sink moves the Malicious Node 22 to neighbourhood trusted Node-16 and link it to Sender Node-10

Fig 5.7 Detect the Malicious Node



Secure Hashing Process Begins in Node 3
Sender Node-11 checks the New Receiver Node-5 and Forward the Packet
Sender Node-25 checks the New Receiver Node-21 and Forward the Packet

Fig 5.8 Dynamic Watchdog Algorithm

CONCLUSION

A critical complement to security mechanisms trusts systems are widely applied to protect MANETs from being attacked by trust sensor node. Those nodes can bypass traditional security protections using their trust identities, but can be possibly captured by trust systems due to their poor reputation or past misbehavior. For this issue this paper proposed a watchdog optimizing technique in two levels. First level of optimization is watchdog location optimizing. This algorithm can find a set of watchdog nodes by considering those nodes locations in a probabilistic manner and to create shortest path between source node and destination node. Then Second level of Dynamic watchdog optimization Technique algorithm to detect the malicious node and estimate energy units for each node.

REFERENCES

[1] Raya, M., Manshaei, M.H., Félegyhazi, M., et al.: ‘Revocation games in ephemeral networks’. Proc. of ACM Conf. on Computer and Communications Security, 2008, pp. 199–210

[2] Bilogrevic, I., Manshaei, H., Raya, M., et al.: ‘Optimal revocations in ephemeral networks: a game-theoretic framework’. Proc. of the Eighth Int.

[3] C. Shields and B. N. Levine, .A protocol for anonymous communication over the Internet,. in *Proc. ACM CCS.00*, pp. 33-42, 2000.

[4] M. Rennhard and B. Plattner, .Introducing MorphMix: peer-to-peer based anonymous Internet usage with collusion detection,. in *Proc. ACM Workshop on Privacy in the Electronic Society*, pp. 91-102, 2002.

[5] Indhu Lekha, S.J., Kathiroli, R.: ‘Trust based certificate revocation of malicious nodes in MANET’. IEEE ICACCCT’2014, 2014, pp. 1185–1189

[6] N. Aravinthan, “certificate revocation scheme based on weighted voting game and rational secure multiparty computing”

[7] Waleed S. Alnumay and Uttam Ghosh, “Secure Routing and Data Transmission in Mobile Ad Hoc Networks”

[8] Kartik Kumar Srivastava, “Secure Data Transmission in MANET Routing Protocol”

[9] Jie Wu, and Abdallah Khreishah. "Network coding techniques for wireless and sensor networks." (2013).

[10] Kim, S.: ‘Trust based dynamic bandwidth allocation scheme for Ethernet passive optical networks’, Wirel. Pers. Commun., 2015, 83, (4), pp. 2869–2882.

[11] Y. Sun, T. La Porta, and P. Kermani, “A flexible privacy enhanced location-based services system framework and practice,” *IEEE Trans. Mobile Comput.*, vol. 8, no. 3, pp. 304–321, Mar. 2009.

[12] K. Liu, J. Deng, P. K. Varshney, and K. Balakrishnan, “Anacknowledgment-based approach for the detection of routing misbehavior in MANETs,” IEEE Trans. Mobile Comput., vol. 6, no. 5, pp. 536–550, May 2007.

[13] Sungwook Kim, “Effective certificate revocation scheme based on weighted voting game approach”.

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