Clustering the nodes with trust value of intrusion detection using iterative process of watchdog mechanism

Jeevitha.T
PG scholar
Dept. of information technology
SNS College of Technology
it.jeevi@gmail.com

Kalimuthu.M
Assoc. Professor
Dept. of information technology
SNS College of technology
mkmuthu73@gmail.com

Sengottuvelan.P
Assoc. Professor
Dept. of information technology
Bannari Institute of technology
sengottuvelan@rediffmail.com

ABSTRACT: DTN (delay tolerant networks) is important field in wireless communication and network security which is emerging as vehicular, underwater and satellite networks. Finally they say it as end-to-end communication latency and the lack of end-to-end path from source to destination. So these characters have several challenges to the security to DTNs. Because of these character by byzantine attacks in which one or more legitimate nodes have been compromised and fully controlled by adversary and cause damage to the network in terms of latency and data availability. Then finally they introduced ITRM for iterative malicious node detection mechanisms for DTNs. They proposed graph based iterative algorithm motivated by the prior success of message passing techniques for decoding low-density parity-check code over bipartite graphs. Form that they improve high data availability and packet-delivery ratio with low latency in DTNs under various adversary attacks which attempt to trust detection scheme and packet delivery control. But the problem of after five iterative checking process the detection and checking time will get slow, so its lead to delay packet delivery ratio. To end this exponentially weighted moving average (EWMA) is employed for nodal contact probability based on function including sync (), leave (), join () are devised for cluster formation and gateway selection. The gateway nodes exchange their network information and perform routing operation. This simulation carried out to evaluate the effectiveness and efficiency of proposed cluster-based routing protocol and this simulation achieves higher delivery ratio and lower overhead and end-to-end delay compared with its non-clustering. And also including intrusion detection for detect the malicious nodes by alarm return type and trust value evaluation.

Keywords: Mobile Computing, Wireless Sensor Network, Intrusion Detection, ITRM, Clustering, ADOC.

1. INTRODUCTION

Disruption tolerant networks (DTNs) exploit the intermittent connectivity between mobile nodes to transfer data. Because lack of consistent connectivity between two nodes exchange data only when they move into the transmission range of each other. In DTNs, a node may misbehave by dropping packets even when it has sufficient buffers. Routing misbehavior can be caused by selfish nodes that are unwilling to spend resources such as power and buffer on forwarding packets of others or caused by malicious nodes that drop packets to launch attacks. Routing misbehavior will significantly reduce the packet delivery ratio and waste the resources of the mobile nodes that have carried and forwarded the dropped packets. Disruption tolerant networks (DTNs) exploit the intermittent connectivity between mobile

nodes to transfer data. In DTNs a node may misbehave by dropping packets even when it has enough buffers. Routing misbehavior can be caused by selfish nodes that are unwilling to spend resources such as power and buffer on forwarding packets of others, or caused by malicious nodes that drop packets to launch attacks. Our approach consists of a packet dropping detection scheme and a routing misbehavior mitigation. The misbehaving node is required to generate a *contact record* during each contact and report its previous contact records to the contacted node. Based on the reported contact records, the contacted node detects if the misbehaving node has dropped packets. To detect misreporting, the contacted node also randomly selects a certain number of *witness nodes* for the reported records and sends a summary of each reported record to them when it contacts them. Apply an ITRM with watchdog mechanisms.

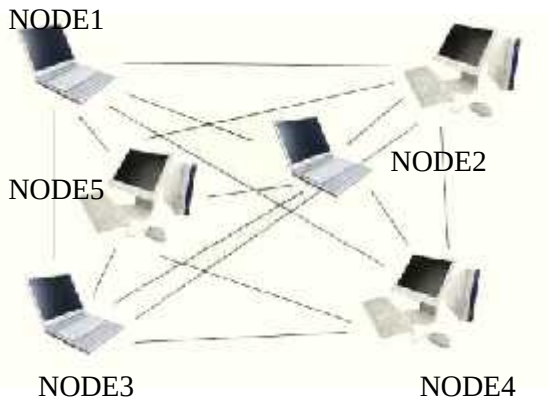

Figure 1: Node Connectivity

A wireless ad hoc network is a decentralized wireless network. The network is ad hoc [9] because it does not rely on a preexisting infrastructure, such as routers in wired networks or access points in managed (infrastructure) wireless networks. Instead, each node participates in routing by forwarding data to other nodes, and so the determination of which nodes forward data is made dynamically based on the network connectivity. Wireless ad hoc networks can be further classified by their application: mobile ad hoc networks (MANETs) wireless mesh networks, wireless sensor networks. Routing is the process of selecting paths in a network to forward the data packets. In packet switching networks, routing directs packet forwarding, the transit of logically addressed packets from their source toward their ultimate destination through intermediate nodes; typically hardware devices called routers, bridges, gateways, firewalls, or switches. Most routing algorithms use only one network path at a time, but multipath routing techniques enable the use of multiple alternative paths. The routing protocol [2] specifies how routers in a network share information with each other and report changes. The routing protocol enables a network to make dynamic adjustments to its conditions, so routing decisions do not have to be predetermined and static. A routing protocol shares this information first among immediate neighbors, and then throughout the network. Proactive, reactive and hybrid are the routing protocol used.

Classification of Attacks on MANETs

- Application Layer: Malicious code, Repudiation
- Transport Layer: Session hijacking, Flooding
- Network Layer: Sybil, Flooding, Black Hole, Grey Hole. Worm Hole, Link Spoofing, Link Withholding, Location disclosure etc.
- Data Link/MAC: Malicious Behavior, Selfish Behavior, Active, Passive, Internal External
- Physical: Interference, Traffic Jamming, Eavesdropping.

2. LITERATURE SURVEY

2.1 An Iterative Algorithm for Trust Management and Adversary Detection for Delay-Tolerant network

Delay/Disruption Tolerant Networks (DTNs)[2] have been identified as one of the key areas in the field of wireless sensor network and communication, where in sparseness and delay are particularly high and they are emerging as promising technology in vehicular, planetary, military/tactical, disaster response, underwater and satellite networks. DTNs are characterized by a large end-to-end communication latency and the lack of end-to-end path from a source to its destination. Applying ITRM to DTNs for various mobility models, we observed that the proposed iterative reputation management scheme is far more effective than well-known reputation management techniques such as the Bayesian framework and Eigen Trust. Further concluded that the proposed scheme provides high data availability and packet-delivery ratio with low latency in DTNs under various adversary attacks which attempt to both undermine the trust and detection scheme and the packet delivery protocol.

2.2 Clustering and Cluster-Based Routing Protocol for Delay Tolerant Mobile Network

An exponentially weighted moving average (EWMA) scheme [5] is employed for on-line updating nodal contact probability, with its mean proven to converge to the true contact probability. Based on nodal contact probabilities, a set of functions including *Sync (), Leave (),* and *Join ()* are devised for cluster formation and gateway selection. Finally, the gateway nodes exchange network information and perform routing. Extensive simulations are carried out to evaluate the effectiveness and efficiency of the proposed cluster-based routing protocol. The simulation results show that it achieves higher delivery ratio and significantly lower overhead and end-to-end delay compared with its non-clustering.

2.3 Trust Management and Adversary Detection for Delay Tolerant Networks

The most famous and primitive global reputation system [2] is the one that is used in eBay. Other well-known websites such as Amazon, Epinions are use more advanced reputation mechanisms than eBay. Their reputation mechanisms compute the average of the received ratings to evaluate the global reputation of a product. Hence, these schemes are vulnerable to collaborative attacks by malicious peers. Use of the Bayesian Approach is also proposed. Finally they proposed *Cluster Filtering* method for reputation. Different from the existing schemes, ITRM algorithm is a graph based iterative algorithm motivated by the previous success on iterative message passing techniques. And also have acknowledgement like key passages are used.

2.4 Defending selective forwarding attacks in WMS

An algorithm to defend against selective forwarding attacks based on AODV routing protocol [7]. The first phase of the algorithm is *Counter-Threshold Based* and uses the detection threshold and packet counter to identify the attacks and the second phase is *Query-Based* and uses acknowledgment from the intermediate nodes to localize the attacker. The simulation results to illustrate the efficiency of the proposed algorithm. This is the first paper to present an algorithm for defending selective forwarding attacks in WMN.

2.5 security design with malicious node detection

In distributed wireless sensor network always have problem in prevention and detection of malicious nodes. So combine the usage of dynamic authentication scheme, primary security design, intrusion detection modules. Here with the intrusion module using alarm return type, trust value calculation and black & white list process are used.

3. EXISTING SYSTEM

DTNs are sparseness and delays are particularly high. In MANET the end-to-end paths through contemporaneous links is assumed in spite of nodal mobility. The disruption is temporary and same path or alternative path is restored quickly, the intermediate contacts between nodes leading to multiple path for transmitting packets to the destination. DTNs have lack of end-to-end communication link so they add ITRM to identify the byzantine nodes with short period of time. These methods have watchdog mechanism for showing the past experience of the node. From that they can analysis the byzantine node and taking the shortest path to reach the destination from the source. Applying ITRM to DTNs for various mobility models observed that the proposed iterative reputation management scheme is far more effective than well-known reputation management techniques such as the Bayesian framework and Eigen Trust. Further, we concluded that the proposed scheme provides high data availability and packet-delivery ratio with low latency in DTNs under various adversary attacks which attempt to both undermine the trust and detection scheme and the packet delivery protocol. ITRM (iterative method for trust and reputation management) is for malicious node detection scheme with the highest strength are detected with higher probability. After 5 iterative processes its gets slow so we proposing. In this figure1 the white line is denoted as path that preferred to send packets to destination, the remaining lines are byzantine path we can do the process by using watchdog mechanism. In that it always stores the past experience of the nearby nodes. Whenever the source try to send the packets to the destination means first it will check processes of watchdog mechanism with ITRM- is a iterative process of identifying the byzantine attacks in nearby nodes like bad mouthing and ballot stuffing. Malicious node attacks on both the network communication and security mechanisms at the same time. Malicious nodes will drop the legitimate packets they have received from realisable nodes and generate their own flows to deliver to other nodes (malicious). So automatically the legitimate node decreases their network performance process. The network performance means data availability and packet deliver ratio. Random waypoint and levy-walk mobility models are used for DTN simulation. Random waypoint model produces exponentially decaying intercontact time distributions to the network nodes making the mobility analysis tractable. Each node is in initial location and travels at constant speed to a random destination. After reaching the destination node may pause for a random amount of time before the new destination and speed are chosen random for the next movement. On other hand of levy-weight is produce power-law distribution that mainly used for animal pattern and now using promising model for human mobility. In this each movement length and pause time distributions closely match truncated power-law distributions and the angles are pulled into uniform distribution. It performs the implementation based on 4 steps. They are movement length, direction, movement time and pause time. ITRM using for identifying the byzantine nodes using rating table of 0 &1.

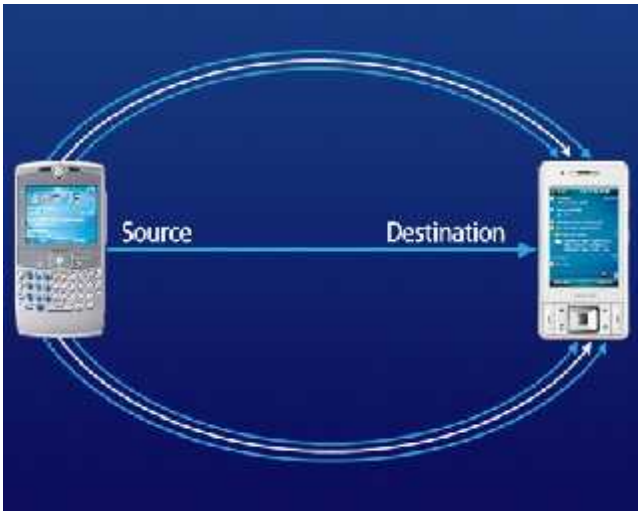

Figure 2: Process of Watchdog Mechanism in ITRM

They provide evaluation only for the bad mouthing on detection scheme and ballot stuffing on trust management. Simulation results hold for ballot stuffing and combination of both bad mouthing and ballot stuffing. It provides a very efficient trust management and malicious node detection mechanisms for DTNs under the threat model and resiliency to a high fraction of malicious nodes and each network nodes accurately compute the reputation values in a short time. This feature is crucial issue in DTNs because of their unique characteristics. It have watchdog mechanism which store the past experience of the node, from that it can identify the byzantine nodes. Then find the shortest path in remaining nodes to reach the destination from source. ITRM significantly outperforms the voting technique by providing success rates in shorter time. Bayesian framework and Eigen Trust is used for the voting techniques. They proposed this mechanisms for provides high data availability with low information latency by detecting and isolating the malicious nodes with low time consumption.

3. Proposed system

In proposed system the ITRM with key passing technique and cluster formation with gateway selection. Exponentially weighted moving average (EWMA) scheme is employed for on-line updating nodal contact probability with its mean proven to converge to the true contact probability. Based on nodal contact probabilities functions including *Sync ()*, *Leave ()* and *Join ()* for cluster formation and gateway selection. The nodes exchange network information and perform routing operation. Then Extensive simulations are carried out to evaluate the effectiveness and efficiency of the proposed cluster-based routing protocol. The simulation results achieve higher delivery ratio and significantly lower overhead and end-to-end delay compared with its non-clustering. It provides a very useful, efficient trust management and malicious node detection mechanisms for DTNs under the threat model and resiliency to a high fraction of malicious nodes and each network nodes accurately compute the reputation values in a short time. This feature is crucial issue in DTNs because of their unique characteristics. It has watchdog mechanism which store the past experience of the node, from that it can identify the byzantine nodes. Then find the shortest path in remaining nodes to reach the destination from source. ITRM significantly outperforms the voting technique by providing success rates in shorter time. Bayesian framework and Eigen Trust is used for the voting techniques. They proposed this mechanisms for provides high data availability with low information latency by detecting and isolating the malicious nodes with low time consumption. Due to the bad mouthing and ballot stuffing random attacks a judge node must wait for a definite number of feedbacks to give its verdict about a suspect node with a high confidence DTN and ITRM are combinable used for transferring the data

from source to destination Key passage method is mainly focused prevention and protection for current position of byzantine attacks. Presenting an algorithm to defend against selective forwarding attacks based on AODV routing protocol. In phase-1 the algorithm *Counter-Threshold Based* and uses the detection threshold and packet counter to identify the attacks and the second phase is *Query-Based* uses acknowledgment from the intermediate nodes to localize the attacker. The gateway nodes exchange network information and it's performing the routing. Extensive simulations are carried out to evaluate the effectiveness and efficiency of the proposed cluster-based routing protocol. Simulation results show the achievement of higher delivery ratio significantly lower overhead and have an end-to-end delay compared with its non-clustering. The Cluster Member with Low Contact Probability included for node detecting to transfer. Node waits for three possible events are slot-timeout, meet-a-node and gateway-outdate. Four challenges are used in clustering. So combine the usage of dynamic authentication scheme, primary security design, intrusion detection modules. Here with the intrusion module using alarm return type, trust value calculation and black & white list process are used. They are

1. Online Estimation of Contact Probabilities
2. Fractional Clusters
3. Inconsistent Cluster Membership and Gateway Selection.
4. Cluster Member with Low Contact Probability

3.1 Simulation

In the first simulation set the number of nodes to be 50 and the data generation rate is 0.1, the clustering threshold is 0.6, and the gateway threshold is 0.1. Every node have the same maximum queue size which varies from 20-200 during the simulation our cluster-based routing protocol yields much higher overall delivery ratio.

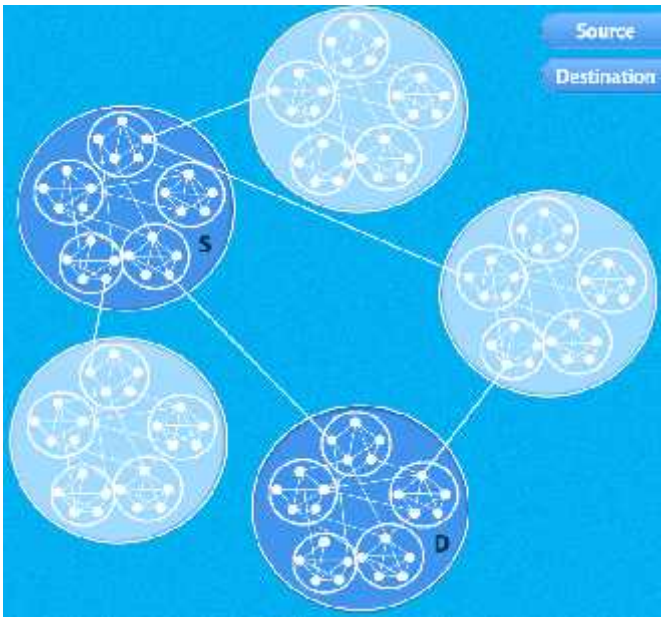

Figure 3: Cluster Formation and Passes the Packet

The higher delivery ratio is due to several reasons including for load balancing implementation. When the queue of a node is almost full then it will ask other Members in the cluster to carry some of its data messages and resulting in low drop rate at each single node. The end-to-end delay of a message in Prophet is increasing almost linearly with the increase of queue size. While cluster-based routing protocol gives shorter delay and the increment is very slower with the long queue size. The reason lies on the difference in message forwarding mechanisms. In Prophet a node always forwards its data message to the meeting node if it has higher delivery probability to the destination of that message even though its own probability is high to that destination. The message arriving at the new node needs to be queued again and leading to longer queuing time in total. In cluster-based routing if the node has high probability to

meet the destination of the message, it will wait for a direct transmission in intra-cluster routing to save the queuing time. The cluster-based routing protocol is varying the number of nodes and the data message generation rate fixing the queue size to 100. The protocols increase their delivery ratio when network density increases. With more nodes in network the traffic load is higher and potentially leading to bottlenecks at some nodes and thus degrading the network performance. If the network is balancing the more nodes and the routes to deliver the messages improving network performance. However balancing mechanism the delivery ratio of cluster-based routing protocol is always much higher compare to normal one. The study of thresholds used in the protocols. γ And $\hat{\gamma}$ are two critical parameters in our cluster-based routing protocol for cluster formation and gateway selection. In general the optimization of γ and $\hat{\gamma}$ is a challenging and complicated problem several parameters such as traffic load, data queue size and the nodal contact probabilities. The Random destination is chosen for each message. Repeat the each simulation for 5 times and show the average results. Each simulation run the simulation time is 10000 seconds and the warm up time is 500 seconds. Our cluster-based protocol needs the warm-up period to form clusters. Exponentially weighted moving average (EWMA) scheme is proven to converge to the true contact probability. Based on the contact probabilities a set of functions including *Sync ()*, *Leave ()* and *Join ()* has been devised for cluster formation and gateway selection in figure (2). The authentication mechanism mainly for the packets are generated by a specific source is provided by a Bloom filter and ID-based signature (IBS). The feedback of the mechanism to determine the entries in rating table is based on a 3-hop loop. In clustering we communicate to other cluster through cluster head and we can identify the destination easily and also finally the packet delivery ratio also increases successfully. Voting technique will find the byzantine attacks in nodes and also malicious node easily with the help of iterative process. We can make the cluster by energy level checking process and making cluster with related one. The energy can calculate by EWMA process. Figure (2) show the overall process. A node with a very low nodal contact probability may still appear in the member list of another node. The main reason is a mobile node may change its mobility pattern in real-life applications. The possible solution for this problem is to use timeout for membership binding.

1) Slot-Timeout Event: Update Contact Probability*:* A *Slot-Timeout* event is generated by the end of every time slot and triggering the process of updating the contact probabilities by using the EWMA scheme. Once the contact probabilities are updated and the *Gateway Update ()* procedure is invoked to update the gateway table. The gateway table maintains a list of gateways to each cluster. Since Node i has updated its contact probabilities to all nodes and potentially choose better gateways. During this procedure the three cases are considered:

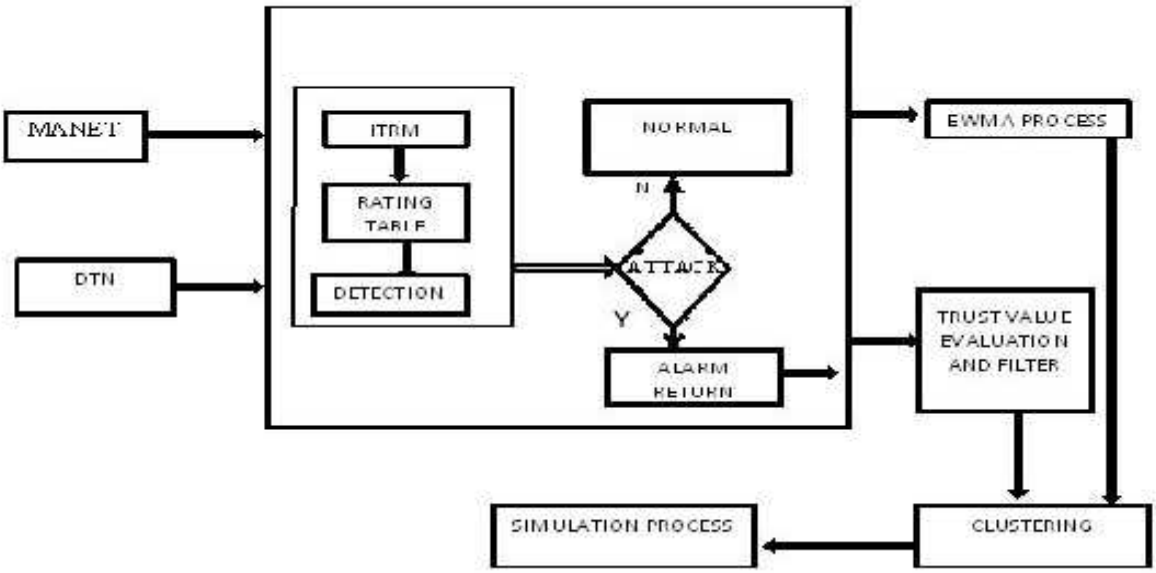

Figure 4: overall process diagram

1) Consider an entry in the gateway table 2) Still consider an entry for Cluster c in the gateway Table

3) Node i also checks the cluster table for possible new clusters not included in its current gateway table. If a new cluster is found then it will be added into the gateway table.

2) Meet-A-Node

The meet-a-node event is generated based on receiving the Hello message (exchanged between two meeting nodes, i and j).

Synchronization of Gateways: Nodes i and j may have different gateways to the same clusters in their gateway tables. The synchronization is needed to keep the "better" one with the higher contact probability. For each of the clusters having high contact probability and the node whichever have lower contact probability gives up and updates its gateway table.

Synchronization of Cluster Members: The clustering of node is distributed and the 2 Node will be maintained the different cluster information before the clustering process is converged. The idea of synchronization is to update the membership based on the latest information of Nodes i and j.

3) Gateway-Outdate Event *RESET*: When the Time Stamp of any entry in the gateway table is older than a threshold Δ; a Gateway-Outdate Event is generated for that entry. Clustering in DTN is unique and non-trivial because the network is not fully connected with node. Due to the lack of continuous communication the mobile nodes may have inconsistent information and they are responding differently. Thus the result it becomes challenging to acquire necessary information to form clusters and ensure their convergence and stability. Although it largely understood by the research community that clustering helps to improve network scalability, no previous work has been done in such emerging unique networks.

3.2 Clustering and routing

Clustering the nodes by using process of EWMA (exponential weighted moving average). Through this can calculate the energy make the related nearby nodes together and make cluster.

3.2.1 Intra cluster routing

If node 1 and 2 are in same cluster then the entire cluster have high contact probability, direct transmission is here. Node 1 transmits the data message only when it meets node 2. No relay node is involved in such intra-cluster routing.

3.2.2 one-hop intra-cluster routing

Node 1 looks up its gateway table if entry found means the node 1 send data to node2 through gateway by using the cluster ID.

3.2.3 Multi-hop intra-cluster routing

Here we can connect many nodes through clustering.

4. Detection Performance

We analytically obtained the waiting time of a judge node before executing ITRM and evaluated the effects of attacks on the detection scheme for a network of size N in which the inter-contact time between the 2 particular nodes. We evaluated the performance of ITRM for different pairs we compared ITRM with the well-known Voting Technique in which a judge node decides on the type of a suspect based on the majority of the votes for that node. In the Voting Technique utilizing the ITRM a judge node decides on the type of a suspect node based on the majority of feedbacks it received.

5. CONCLUSION

We have investigates the DTN for delivery and using ITRM for previous checking by using watchdog mechanisms. It has the problem which lack of checking process after 5 iterative checking. Cluster based routing protocol with EWMA is introduced for improving the packet delivery ratio and also the reduction of packet drop. Once the clustering procedure is finished the each node in the network is associated with a cluster. For any two clusters the members have high enough contact probability a pair of gateway nodes are identified to bridge them. The gateway nodes exchange network information and perform the routing. Extensive simulations are carried out to evaluate the efficiency of cluster-based routing.

6. Future enhancement

ITRM Key Passage method is newly introduced for security on current node while passing the packet. One node of the simulation result is considered as a ITRM which passes the key to the paths from source to destination. First the intermediate node will passes the key request to the legitimate nodes and after getting the response only it passes the data to intermediate nodes. And can use security design with primary security by the process of dynamic authentication, pairwise key establishment, broadcast authentication establishment. In clustering includes that transmission and monitoring scheduling which helps to reduce the traffic in network with the help of member node(MN), cluster head(CH) using a protocol of secCBSC(Secure Cluster based Communication protocol) performance evaluation to reduce overhead by storage, computation and communication overhead process.

7. REFERENCES

[1] K. Fall, “A delay-tolerant network architecture for challenged Internets,” in *Proc. ACM SIGCOMM*, pp. 27–34, 2003

[2] An Iterative Algorithm for Trust Management and Adversary Detection for Delay-Tolerant Networks Erman Ayday, Student Member, IEEE, and Faramarz Fekri, Senior Member, IEEE 2012

[3] E. Ayday, H. Lee, and F. Fekri, “An Iterative Algorithm for Trust and Reputation

Management," Proc. IEEE Int'l Symp. Information Theory (ISIT '09), 2009.

[4] E. Ayday and F. Fekri, "A Protocol for Data Availability in Mobile Ad-Hoc Networks in the Presence of Insider Attacks," Elsevier Ad Hoc Networks, vol. 8, no. 2, pp. 181-192, Mar. 2010.

[5] Clustering and Cluster-Based Routing Protocol for Delay-Tolerant Mobile Networks Ha Dan and Hongyi Wu, *Member, IEEE 2010*.

[6] A. Jøsang, R. Ismail, and C. Boyd, "A Survey of Trust and Reputation Systems for Online Service Provision," Decision Support Systems, vol. 43, no. 2, pp. 618-644, 2007

[7] Defending Selective Forwarding Attacks in WMNs Devu Manikantan Shila (*Student Member, IEEE*), Tricha Anjali (*Member, IEEE*) Department of Electrical and Computer Engineering Illinois Institute of Technology Chicago.

[8] Bin Xiaoa,∗, BoYua,b, Chuanshan Gaoc CHEMAS: Identify suspect nodes in selective forwarding attacks 2007.

[9] Performance Comparison of Multi-Hop Wireless Ad Hoc Network Routing Protocols," Proc. ACM MobiCom,pp.85-97,1998.

[10] Adaptive Security Design with Malicious Node Detection in Cluster Based Sensor Networks meng-yen hsiegh, yueh-min huang, han-chieh chao, 29 april 2009.