International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 25 Issue 9 – AUGUST 2018.

TRUST MESSAGE AUTHENTICATION CODE FOR ENHANCING THE ROUTING SECURITY OF MANETS

K. TAMILARASI [#1]

[#] *PRINCIPAL,DEPARTMENT OF COMPUTER SCIENCE,SRI JAYAJOTHI ARTS AND SCIENCE COLLEGE, THARAMANGALAM, SALEM, India*

***Abstract*— In this paper trust values should be calculated to find neighbor nodes for each and every node in the networks. Trusted nodes will be used to communicate with the routes and no ACK process is used, so it takes less time for communication. Cryptographic techniques are used to reduce the network overhead caused by digital signature. Key exchange mechanisms will be used to eliminate keys and it is more secure because of key generation concept is introduced it is energy efficient model. Light weight Intrusion detection system is used for estimating the trust and consumes limited computational resources. The performance will be evaluated in the software simulation**

***Index Terms*— Acknowledgement (ACK); Trust system; Mobile Ad hoc NETwork (MANET)**

I. INTRODUCTION

A Mobile Adhoc Network (MANET) is an infrastructure less network capable of communicating with all the nodes in the networks.The routers are used to move randomly so that the networks wireless topology changes rapidly and unpredictably. Minimal configuration and quick deployment are enough to make adhoc networks which are suitable for emergency situations especially in the military conflicts and medical situations. To discover routes between all nodes in the networks routing protocols will be used. Route establishment will be made between a pair of nodes so that all messages will be delivered in a timely manner. Route Construction is used to minimize the overhead and bandwidth consumption. The routing table will keep routing table as small, choose the best routes for destination, keep table up to date even when node die or it can move or join in the network and it requires a small amount of messages. The advantages of MANET are 1) Low cost of deployment 2) Fast deployment 3) Dynamic configurations. Ad hoc networks not have a priori knowledge of topology of network around them. The idea is that a new node will be announces its presence and listening to its neighbors. The MANET is capable of creating a self–forming, self-maintained and self-healing used for network flexibility. Data packets are used to hop from one to another for network coverage and mainly used to overcome non Line Of Sight (LOS). MANET routing protocols can have:1) Proactive protocol 2) Reactive protocol. Proactive protocol are used to maintain consistent and updated routing information for each and every pair of network nodes route will be updated at time intervals. Reactive protocol is used to establish the route to a destination and route request will be initiated with the help of route discovery process.

Energy constrained operation will be used because of batteries will be used for mobile node and have a limited power supply additional to that processing power also to be limited in it. Issues is that each and every node will be acts as an end systems and a router at the same time but it requires additional energy to forward packets to other nodes. The network topology also uses multi-hop can change it frequently in which routes also changes, packet losses and network partitions will be occurred frequently and no default router will be used in this for sharing of information because each and every node will be acts as a router.

The node behavior is to be classified based on the routing functionality nodes which cannot drop packets while forwarding packets. Misbehaving nodes can be classified as: 1) Selfish or malicious nodes where all nodes are not participating in the packet forwarding function. Selfish node can drop all packets. Malicious node misbehavior is usually greater than that of selfish node misbehavior.

Detection of infected routes is used to reduce the misbehavior impact but it is not fully eliminate the misbehavior impact. To eliminate the misbehavior impact to detect selfish nodes on infected routes two approaches will be used:1) Centralized approach 2) Localized approach. Centralized approach is that central authority to detect nodes misbehavior and report will be generated by routes then the user will identified as infected .Localized approach knows about the infected nodes and also knows the next hop neighbors details.

Key generation mechanism will be used for more secure communication. Diffie-Hellman algorithm will be used to transfer the packets more securely. Exchanging of information also in secret way and establishing a shared secret key. The rest of the paper organized as follows. In Section II discuss about related work and contrast with existing work .In Section III is about Architecture model .In Section III discussed about modules .In Section IV is about Algorithms for Diffie-Hellman. Finally in Section V is about conclusion and future work.

II. RELATED WORK

Intrusion Detection System concept will be used in MANET to eliminate the intruder in the node but it is difficult to develop intrusion detection system especially in MANETS. In [2], Security is difficult to maintain in the MANET than in the wired network. Vulnerabilities in Mobile Adhoc networks are free to join in the network and it does not provide secure boundary to protect the dangers in the network. Mobile nodes can join or leave the network anytime so that malicious nodes cannot be prevented. Threats in the nodes are also dangerous than outside network and this also not easy to detect. In [3], Denial Of Service (DOS) is used to prevent the attacks. Attacker can send a large amount of requests to a server even in the absence of central router nodes also have to trust each other. It is vulnerable to misbehaviors for several reasons: 1) Misbehavior of faulty nodes due to hardware errors.2) valuable information are to be extracted from network. In [4], Intrusion Detection is used to process and monitor the system and this is achieved by using Intrusion Detection system (IDS) once it can detect the attack it generates an alarm to the administrator. Neighbor IDS can use the intrusion detection and fault tolerance will be used to recover from losses .The mobile agents is used to reduce the the power consumption.

In [5], Exchange of routing information is used to discover a new route to deliver a packet to destination. Lower routing overhead has bandwidth and battery power used to deliver data thus reducing the routing packets for authentication and reduces overhead for security. In [6], Dynamic source routing is to reduce the network overhead from the route discoveries. once the host sends an packet to the same host .Route error packets are returned from the original sender. In [7], Isolate the misbehaving nodes from the routing protocols in the networks so that trust based routing mechanism will be used to detect and identify the malicious node. Network Intrusion Detection System is used to detect the attacks and is also acts as a pathway for intrusion. Signature based intrusion detection system is used to give alert to the entire networks. Acknowledged packets are encrypted to provide integrity using 3GPP algorithm.

In [8], Malicious node actions will be protected by Authenticated Routing for Adhoc Networks (ARAN) cryptographic certificates also use in it. Source node is used to sign the routing messages and it will be broadcast to neighbors. Cost will be high for computing resources and the authenticity of packets are to be checked with Secure Efficient Adhoc Network (SEAD) by hash chain used to update routing information shared secret key is used for authentication.Asymmetric keys are used to distribute the state information attacks will be reduces because of priority ranking from the neighbor nodes based on the traffic in Secure Link State Routing Protocol (SLSP).Shared key is used to establish the Security Association (SA).

In [9], Multipath routing and trust with encryption technologies. Suspected nodes have a high power and the trust values use the combination of derived trust and reputation. Hybrid routing protocols which are used for low storage, higher mobility and availability of routes. In [10], The attackers can obtain the information easily because of the insecure protocols. STAR is used to reduce the routing overhead by using Least Overhead Routing Approach(LORA).Source Tree should be maintained to update tables and no periodic messages are required.FSR is used to update messages are reduces the size by updating network information for nearby nodes at a higher frequency. The Cluster Head Gateway Switch Routing Protocol uses the concept of hierarchical network topology and routers will be discovered using the reactive protocol.

No periodic updates are used but the routing protocol information is needed in this compare with the bandwidth and its counterparts. Implementation is independent for different operating systems large amount of time is wasted for finding routes.

III. ARCHITECTURE MODEL

The Architecture model (fig A) all nodes are in the networks, trust systems are used to update neighbor details to check whether the malicious nodes is present or not if malicious nodes are not present it can discover the route to send the data from source to destination then key will be generated for both sender and receiver a secret key will be shared between two nodes for communication if the key will be same then data will be transferred to the destination.

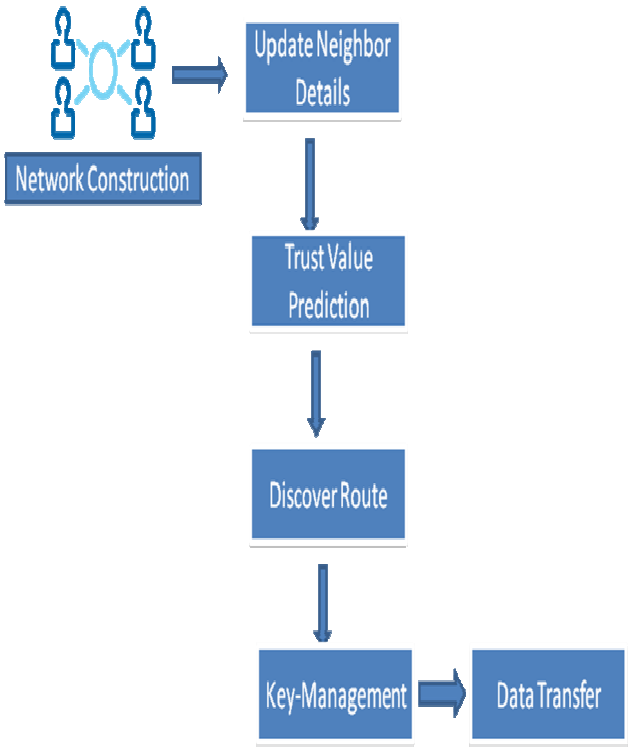

Figure: A. Architecture design

A .Topology construction

Topology will be constructed for a Mobile Adhoc Network with set of nodes the each nodes will be evaluated based on the capacity with respect to network parameters and this is used to identify each nodes neighbor.

B.Trust value prediction

Trust values are to be calculated on the basis of both physical and logical methods. The physical trust model is evaluated with the help of node details obtained in the previous model and the logical model applies affinity and trustworthy values which are used to identify whether the neighbor is trusted node or not. After calculating those values, trusted nodes list is generated and the new route to destination is discovered.

C.Key management

After identifying the route, the sender establishes a key-management scheme to make system more secure.Queries can be issued by a user and can be issued anywhere in HWSN through a nearby CH.A CH which takes a query to process is called query processing center(PC) and source redundancy by which m_s SNs sensing a physical phenomenon in the same feature zone are used to forward sensing data to their CH node. Path redundancy by which m paths are used to relay packets from the source CH to the PC through intermediate CHs.

E. Distributed Voting Mechanism:

Every CH also creates a pair wise key with every other CH thus a pair wise key exists for secure communication between nodes. To remove malicious nodes from the system a voting -based distributed IDS is applied periodically in every minute interval. A CH is being accessed its neighbor CHs, and a SN is being accessed by its neighbor SNs.In each interval, m neighbor nodes (at the CH or SN level) around a target node. Collecting the votes based on their host IDS results to collectively decide if the target node is still a good node.

F. Trust Evaluation:

Trust enables a subset of the nodes to evaluate the behavior of neighboring nodes and make decision about them. Trust values are usually obtained taking into considerations different parameters such as personal reference also known as direct trust and also getting recommendations from the neighboring nodes i.e. reference also known as indirect trust and these parameters provided us a better assessment of trustworthiness.

G Assessment:

Performance of algorithm is evaluated by using graph representation. It shows that proposed framework is able to adopt to changes in time parameters values while other approaches cannot. The performance gap between the proposed framework and other approaches is at the high level compare to other approaches .It provides better flexibility in the query processing center.

IV. ALGORITHMS FOR LIGHT WEIGHT INTRUSION DETECTION SYSTEM

The objective of Light weight intrusion detection System can easily be deployed in any node of a network, with minimal disruptions to operations. Easily be configured by system administrators who need to implement a specific security solution in a short amount of time. It is small, powerful and flexible enough to be used as permanent elements of the network security infrastructure.

In the Detection Algorithm no malicious nodes appear during the initial stage of sensor node deployment.SNs maintains two databases namely: 1) Malicious nodes and 2) Neighbor knowledge in the neighbor knowledge, broadcasting protocols are used to reduce the number of transmissions. And to detect the warm hole attacks in WSNs. In the malicious nodes, malicious counter have suspicious node stored in a CH crosses a threshold x means CHs creates and propagate a new rule to each and every SNs node in cluster. Then SNs update a new rule and add entry to its malicious database and malicious node is isolated from cluster and not involved in communication in the networks.

```
Communication Node
1.    Repeat <listen to the packet>
2.     Check<packet header>
3.      If{ID=destination node's ID}{
4. If Local-Detection (packet)
5.   Then drop (packet)
6.      Else receive (packet);
7.    }
8.    And If (source & destination's ID,1
Hop neighbor)
9.           Then Global detection (packet)
10.    Else Drop (packet)
11.  Until No transmission
```

Fig 2 Algorithms of activating monitor nodes

In fig 2, SNs receives a packet from a sensor in the network. If source node's ID is in its black list then the sender node uses local function () to drop the packet. Both source and destination nodes are one-hop neighbors; triggers the Global-detection function.

```
Global-detection (packet)
1. {
2.  If Looking (packet_i _id, buffer)
3.  Then {
4.    If Check (node's ID, 2 hop neighbor's
5.       List)
6.     Or Check (packet_i, predefined-rules)
7.   Then {
8.          Create (alert);
9.           Send (alert, cluster-head);
10        }
11.  }
```

Fig 3 Global detection at monitor nodes

In fig 3, Global detection modules uses two – hop neighbor Knowledge and routing rules to detect anomalies within their transmission ranges.

V. CONCLUSION AND FUTURE WORK

This paper describes to decrease energy loss and to increase QoS and high security by using pair wise key is used. lifetime of heterogeneous wireless sensor networks is also maximized while satisfying the reliability, timeliness and security requirements in the presence of unreliable wireless communication and malicious nodes .and Trust/reputation management system is also used to strengthen intrusion detection through "Weighted Voting" mechanisms and Finally Light Weight Intrusion Detection System algorithm is the efficient way to detect malicious nodes in networks.

For Future Work, the more efficient trust based system are used, where concurrent query traffic is heavy means trust based admission control is used and to optimize application performance.

REFERENCES

[1] Hamid Al-Hamadi and Ing-Ray Chen, "Redundancy Management of Multipath Routing for Intrusion Tolerance in Heterogeneous Wireless Sensor Networks" IEEE Trans. Networking., vol.10, 2013

[2] jiun-jian liaw,lin-huang chang and hung-chi chu, Improving Lifetime in Heterogeneous Wireless Sensor Networks with The Energy-Efficient Grouping Protocol "In "l J.Inno.Comput.inf. and Ctrl., vol 8,no.9 ,2012.

[3] Kewei Sha,Jegnesh Gehlot and Robert Greve "Multipath Routing Techniques in Wireless Sensor Networks".

[4] Hoseein Jadidoleslamy,"A hierarchical Intrusion Detection Architecture for Wireless Sensor Networks IJNSA, vol.3, no.5, 2011.

[5] F. Bao, I. R. Chen, M. Chang, and J. Cho, "Hierarchical trust Management for Wireless Sensor Networks and its Application to Trust Based Routing and Intrusion Detection",IEEE Trans. Netw. Service Manag., vol.9, no.2,pp ,161-183,2012

[6] C.j Fung,z. jie I.Aib and R. Boutaba. "Drichlet-based Trust Management for Effective Collaborative Intrusion Detection networks", IEEE Trans.Netw.Service Manag., vol.8,no.2,pp.79-91,2011.

[7] S. Ozdemir," Secure and reliable data aggregation for Wireless Sensor networks", Proceedings of the 4th international conference on ubiquitous computing systems, Tokyo, japan, 2007.

[8] Enrique J.Duarate-Melo, Mingyan Liu EECS, University of Michigan,Ann Arbor " Analysis of Heterogeneous Wireless Sensor Networks".

[9] Ping Yi,ting Zhu,Qingquan Zhang,Yue Wu,Jianhua Li "School Of Information Security Engineering, China " Green Firewall: An energy-efficient Intrusion Prevention Mechanism in Wireless Sensor Networks".

[10] Su Man Nam and Tae Ho Cho, "An Energy Efficient Countermeasure against multiple attacks of the false data injection attack and false hello flood attack in the Sensor Networks

[11] Qurat ul-Ain I.Tarriq, Saneeha Ahmed, Huma Zia "An Objective based Classification of Aggregation Techniques for Wireless Sensor Networks.

[12] Hosamsoleman, Ali Payandeh,Nasser Mozayyani, Saeedsedighiankashi "Detection Collision Attacks in Wireless Sensor Networks usingrule-based Packet Flow rate", IJERA vol 3,issue 4,2013.