Authentication Mechanism for Mobile Sink To Access Network in Wireless Sensor Network

*****C.Rajasharavanan**,** #M.Praveen Umar**,**

[*]*PG Scholar Dept of CSE, King College Of Technology, Namakkal*

[#]*M.E., MBA AP/CSE, King College Of Technology, Namakkal*

Abstract

In multihop wireless network security is an important phenomenon .Trust based routing is important than low cost shortest path routing.In this paper a RACE(Report based payment scheme)used for trust based routing.In this RACE based technique no other cryptographic operations used ,it will not increase the processing over head of network.One of the node can be used as accounting center it can identify the cheating node using trust based algorithm . In this evidences of nodes are required to identify the cheating node,it avoids the blindly routing of source node.Routing algorithm makes source node to establish the many trused routes to reach destination node.In this evidences of nodes are required to identify the cheating node. It is a robust efficient approach for the detection of the Black hole attack without any communication overhead.In this multi hop wireless network nodes also take part to route the other nodes packet by implementation of payment scheme.It ensure the cooperative mechanism of nodes and packet transmission is to be regulated,it enforce the fairness of network.

Index Terms: *RACE,Trust based routing , Block hole attack.*

I. INTRODUCTION

The interest in Multi-Hop Wireless Networks (MWN) such as Mobile AdHocNETwork (MANET), Vehicular Ad-Hoc NETwork (VANET), MultiHop Cellular NETwork (MCN), and Wireless Mesh NETwork (WMN) has been increasing significantly. In these networks, the traffic originated from a node is usually relayed through other nodes to the destination. Multi-hop routing packet Can extend the communication range using limited transmit power, improve area Spectral efficiency, and enhance the network throughput and capacity. Moreover, these networks can be deployed more readily and at low deployment costs in developing or rural areas. However, due to involving autonomous devices in packet relay, the routing process suffers from new security challenges that endanger the practical implementation of themultihopwireless networks.Most existing routing protocols assume that the nodes of multihop wireless network are willing to relay other nodes' packets. This assumption is reasonable in disaster recovery and military applications because the nodes belong to a single authority and pursue a common goal, but it may not hold for civilian applications where the nodes are autonomous and aim to maximize their welfare. Although the proper network operation requires the nodes to collaborate, collaboration consumes their valuable resources such as energy and computing power, which stimulates the nodes to behave selfishly. Therefore, in civilian applications, selfish nodes are not voluntarily interested in cooperation without sufficient incentive and make use of the cooperative nodes to relay their packets, which has negative effect on the network fairness, performance, and security. Fairness issue arises when selfish nodes take advantage from the cooperative Nodes without any contribution to the network and The cooperative nodes are unfairly overloaded because the network traffic is concentrated through them. The selfish behaviour also degrades the network performance significantly, which may result in failure of the multihop communication.

Incentive systems are more appropriate for multi-hop wireless networks because in addition to cooperation stimulation, the systems can achieve fairness by charging or rewarding credits to balance between a node's contributions and benefits. A node's contribution can be relaying other node's packets or paying credits, whereas a node's benefit can be relaying its packets or earning credits. Moreover, since the network nodes payfor relaying their packets, incentive systems can discourage resource exhaustion attack where malicious nodes exchange bogus packets to exhaust the intermediate nodes' resources.However, the practicality of the existing incentive systems is questionable because they impose significant overhead cost. Hence, a report based incentive scheme is proposed for multi-hop wireless networks. Initially, the source node establishes a route to the desti nation through opportunistic routing. Then it forwards the packets in the established route. Once a session is over, the nodes submit light weight reports (instead of receipts) to the AC at the end of each session forverification and temporarily store security proofs called Evidences. The reports contain the number of packets relayed and flag bit (indicating whether last relayed packet is data or acknowledgement) without security proofs. Evidences are requested for cheating reports to identify and evict cheating nodes that submit incorrect reports. Thus, the AC verifies the report by investigating its consistency with almost no cryptographic operations or computational overhead.

A Mobile Ad Hoc network consists of wide range of mobile nodes that actively participate in data transmissions. The mobility and network resource constraints of such mobile nodes take part in network partitioning lead to performance degradation. To overcome performance degradation several replication techniques have been proposed. All those techniques consider that all the mobile nodes in the network are actively collaborating in sharing their memory space. But in reality there are some nodes that does not cooperate or partially with other nodes. Such nodes are called selfish nodes. These nodes reduce the data accessibility in network. To overcome this we term selfish replica allocation- examining the impact of selfish node in mobile Ad Hoc networks from the perspective of replica allocation. The notion of network layer capacity and describe capacity achieving power Allocation and routing algorithms for general networks with wireless links and adaptive transmission rates. In optimality, fairness, implementation complexity, and robustness to time varying channel conditions and changing user demands are discussed. Analysis is performed at the packet level and fully considers the queuing dynamics in systems with arbitrary, potentially IV burst, arrival processes. Ad-hoc wireless networks are given special attention. A simple cell partitioned model for a mobile ad-hoc network with N users is constructed, and exact expressions for capacity and delay are derived. End-to-end delay is shown to be O(N), and hence grows large as the size of the network is increased. To reduce delay, a transmission protocol which sends redundant packet information over multiple paths is developed and shown to provide O(pN) delay at the cost of reducing throughput. A fundamental rate delay trade-off curve is established, and the given protocols for achieving O (N) and O (pN) delay are shown to operate on distinct boundary points of this curve.

Multi-hop wireless networks are collections of mobile nodes connected together over a wireless medium. These nodes can freely and dynamically selforganize into arbitrary and temporary, networktopologies, allowing people and devices to seamlessly internetwork in areas with nopreexistingcommunication infrastructure, (e.g., disaster recovery environments).RACE provides secure data forwarding in multihop networks for mobile user using limited transmit power and with fair traffic load.

II. PROPOSED WORK

A report based payment scheme (RACE) is proposed for multihop wireless networks. The RACE where the nodes send light weight payment reports (instead of receipts) to update the credit details and store Evidences which contains the security proofs. Moreover, here reports are sent per session instead of per message. Hence, communication and processing overhead are reduced drastically. The AC verifies the payment by investigating the consistency of the reports, and clears the payment of the fair reports with almost no cryptographic operations or computational overhead.For cheating reports, the Evidences are requested to identify and evict the cheating nodes that submit incorrect reports, e.g., to steal creditsor pay less. In other words, the Evidences are used to resolve disputes when the nodes disagree about the payment. Instead of requesting evidences from all the nodes that are participating, the proposed systemcan identify cheating nodes by submitting and processing few evidences.

In RACE, Evidences are submitted and the AC applies cryptographic operations to verify them only in case of cheating, but the nodes always submit security tokens, e.g., signatures, and the AC always applies cryptographic operations to verify the paym--ent in the existing receipt based schemes. RACE can clear the payment nearly without applying cryptographic operations and with submitting lightweight reports when Evidences are not frequently requested. Moreover, cheating nodes are evicted once they commit one cheating action.RACE is the first payment scheme that can verify the payment by investigating the consistency of the nodes' reports without systematically submitting and processing security tokens and without false accusations.

RACE is also the first scheme that uses the concept of Evidence to secure the payment and requires applying cryptographic operations in clearing the payment only in case of cheating.

A. System Architecture

The outline of the system is presented in Figure I multihop wireless network a source sends packets to destination through number of intermediate nodes. Every node stores report and evidence at the end of each session. An offline trusted party is used which verifies consistency of the report. At the end of each session all the nodes that took place in the communication submit their reports to the offline trusted party. If the report is found to be cheating, then evidences are requested from the corresponding node. If the reports are found to be fair, then the credit accounts are updated respectively. If a cheating node is identified it is evicted from the network.

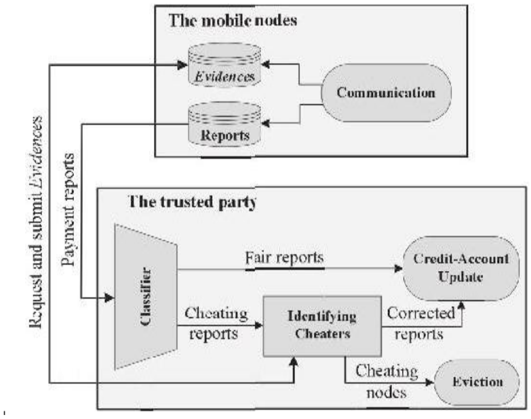


Figure.1 : System Architecture

B. Flow Diagram

The Flow diagram of the proposed system is depicted in Figure 2Initially, all the nodes are involved in communication sessions. Once the source and the destination nodes are identified, the packets reach the destination in multiple hops in established opportnistic routing. The payment reports and evidences are temporarily stored. Thenodes accumulate reports and send them in batch to the AC. Now, the AC classifies the reports into fair and cheating. The AC requests evidences from the nodes that are involved in cheating reports to identify the cheating nodes. The cheating nodes are evicted and the payment reports are corrected

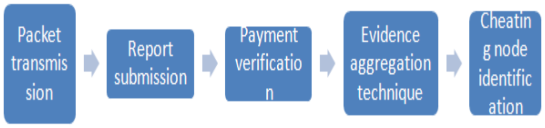


Figure.2: Flowdiagram

C. Modular Design

Modular design defines structure of the overall module. Modularity is a general system method typically defined as a degree to which a system's components may be separated and recombined. The overall system consists of the following modules,

1.Multihop wireless network establishment and node communication

2.Report submission and classification of fair and cheating reports

3.Evidence requisition and node eviction

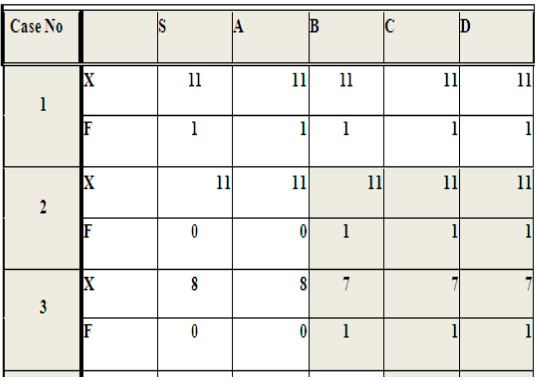
1) Multi-Hop Wireless Network Establishment and Node Communication

Initially, a certain number of mobile nodes are created with an initial locationand a coverage area. Another static node is created that acts as the Accounting Center and maintains a node's credit and debit details and also ensures security. After identifying the source and the destinationnodes and the number of packet s to be sent, the source starts relaying each packet to one of the intermediate nodes. Here, the route establishment is done opportunistically i.e., when there is no path directly from source to the destination, packets are transmitted to the intermediate nodes through multiple hops. The hash chain is generated by iteratively hashing a random value k times where k is the number of packets sent. After the first packet reaches the destination, it sends theacknowledgement in the same route the packet travelled back to the source. Along with the acknowledgement, the destination node also sends the last hash value to each of the intermediate node along that way.
When the second acknowledgement is received, the destination sends the next hash value. Each intermediate node verifies the hash value by making sure that hˆ(X1)is obtained from hashing hˆX. The same process continues until the last packet. The nodes are storeonly the last released hash value for composing the Evidence.

2) Report Submission And Classification Of Fair And Cheating Reports

To provide incentives for the nodes, two things are maintained, namely, report and evidence. The report is a light weight component and contains the number of messages a node has relayed and a flag bit indicating whether the last message If the bit it set to 0, then it is a data and it was an acknowledgement it will be set to 1. The evidence contains the security proof i.e., the last hash value received by a node. The reports are sent once per session to the Accounting Center to claim for payments. The AC verifies and classifies the reports as fair or cheating based on the following cases.If a session is broken during relaying the Xth data packet, the reports of the nodes from S to the last node that received the packet report X and F of zero, but the other nodes report X - 1 and F of one. If a session is broken during relaying the Xth ACK packet, the nodes in the session report X messages, and the nodes from D to the last node that received the ACK report F of one, but the other nodes report F of zero.

The reports are classified as cheating if they do not match one of the case given in Table 1



Case No		S	A	B	C	D
1	X	11	11	11	11	11
	F	1	1	1	1	1
2	X	11	11	11	11	11
	F	0	0	1	1	1
3	X	8	8	7	7	7
	F	0	0	1	1	1

Table .1 Cases of Fair Report

Case 1 is reports for complete session and Cases 2 to 4 are reports for broken sessions. For Case 1, all the nodes report the same number of messages and F of one. For Case 2, the session was broken during relaying the ACK packet number 11 and B is the last node that received the packet. For Case 3, the session was broken during relaying the data packet number 8 and node A is the last node that received the packet. For Case 4, the session was broken during relaying the first data packet, and node B is the last node that received the packet, and therefore nodes C and D did not submit the payment report of the session.

3) Evidence Requisition and Node Eviction

Nodes that do not achieve any one of the aforementioned rules are classifies as cheating. The objective of securing the payment is preventing the attackers (singular of collusive) from stealing credits or paying less, i.e., the attackers should not benefit from their misbehaviours. Three types of attacks have been simulated in order to implement the selfish nodes.

1. Message flooding attack

2. Packet dropping attack

3. False claiming attack

a) Message Flooding Attack

In this type of attack, the attackers send bogus messages to deplete the resources of the intermediate nodes. This will degrade the performance of the network which may even cause the multi-hop to fail. Due to the incentive scheme, as the node creates many messages the credit value of the attacker node will keep decreasing and at a point of time the credit value reaches 0 where the node cannot send further packets. Thus, the incentive scheme acts as a barrier for the attacker to disrupt the network connectivity.

b) Packet Dropping Attack

A packet drop attack is an attack in which a router that is supposed to relay packets instead discards them. This can happen due to many reasons. A malicious node can drop a packet because forwarding the packet will deplete its resources like battery power, bandwidth etc. Since they are routinely dropped in a lossy network, detecting and preventing these attacks is difficult.Here, we can easily find the node that drops the packet from the report. Since the report contains the number of messages that it relayed, the results of the cheating node will be much different from the other nodes. So, the proposed system effectively identifies the node that drops the packet without much computational overhead.

c) False Claiming Attack

False claiming attacks are more common in incentive based networks. Since a node is always autonomous and interested in its own welfare, selfish nodes will try to produce false reports in order to steal credits by claiming that it has relayed more number of messages. This type of attack can be performed by more than one node. Hence, in this case, it is important that the AC processes the Evidence in order to find the cheating node. The AC requests for the last hash value. However, the attacker node will not have it since it has not relayed the number of messages that it has claimed. Thus, the attacker node is found by processing the evidence. Another important point is that, this scheme works with almost no processing overhead because evidences are requested only when a conclusion cannot be arrived by checking the reports.

The AC requests the Evidence only from the node that submits report with more payment instead of all the nodes in the route because it should have the necessary and undeniable proofs (hash chain elements).In this way, the AC can precisely identify the cheating nodes with requesting few Evidences. Once a node is found to be a cheater, it is evicted from the network and cannot participate in further transactions.

Algorithm: RACE

Input: Source node, Destination node, Number of packets.

Output: Identification and eviction of Cheating node and updation of credits.

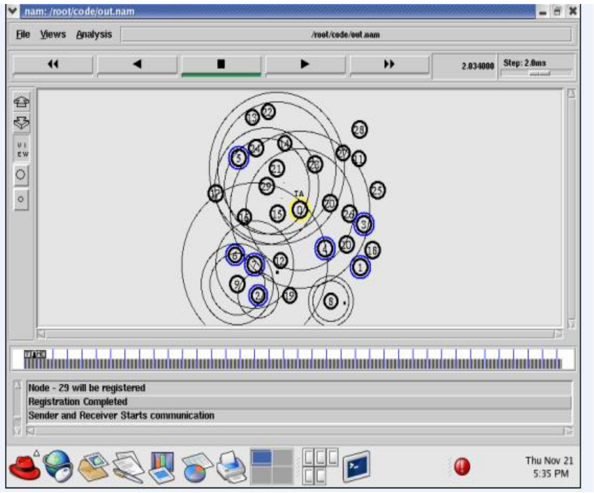
```
//niis the source, intermediate or destination node that is running the algorithm.

if (niis the source node) then

Send (Px) ; //send Pxto first node in the route
```

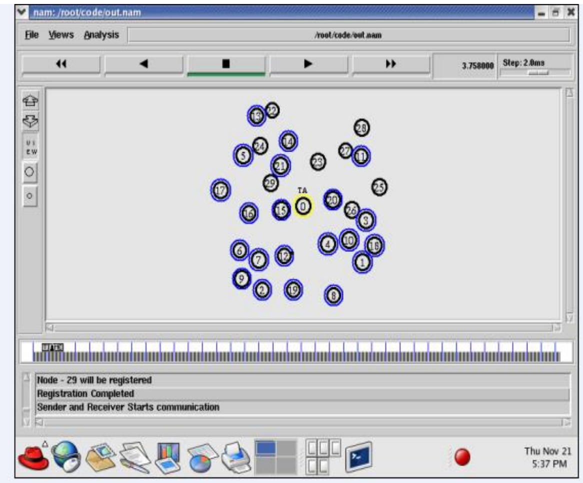
```
else
if (ni is an intermediate node) then Relay the packet;
Compute the number of packets sent and update the flag bit //0 for data and 1 for acknowledgement
end if
if(niis the destination node) then
Send (hx) to all intermediate nodes along with the acknowledgement;
end if else
Drop the packet;
Send error packet to the source node;
end if
end if
if (PX is the last packet) then Report= {X,F}
Evidence={hX}
Store report and evidence; end if;
Submit the reports to the AC per session if(reports are fair) then
Clear the payment
else
Request for the evidence from the suspected nodes
if(Evidence is clear node) then // has the appropriate hash value Clear the payment
end if else
Evict the cheating node from the network
end if
end if
```

D. Screenshots



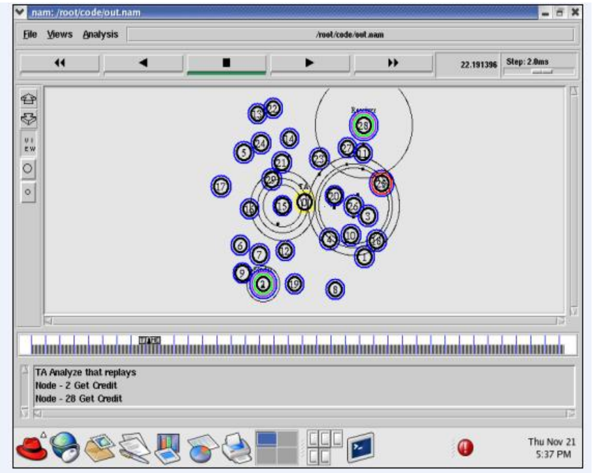
Node - 29 will be registered
Registration Completed
Sender and Receiver Starts communication

Figure.3 Completion of Node Registration



Node - 29 will be registered
Registration Completed
Sender and Receiver Starts communication

Figure.4 Sender and Receiver Starts Communication



TA Analyze that replays
Node - 2 Get Credit
Node - 28 Get Credit

Figure.5Cheating Node Detected.

III. PERFORMANCE EVALUATION

To evaluate the performance of the proposed algorithm, existing environment is compared to that of the proposed environment by performing the message flooding attack. That is depicted using graph of how the network's performance is affected with and without the credit scheme. To facilitate this, the energy level of the intermediate node is considered.The main aim of the source node's flooding behaviour is to deplete the intermediate node's resources. In essence, the energy of the node will drop drastically. So, if there are no credit schemes, then there is no policy to stop this flooding attack and hence the energy of the node will drop drastically for a particular simulation time. But in case of the credit scheme, there is a policy adopted to stop flooding. That is, when there are no enough credits, then the attacker can no longer send packets. Thus, it is clear that the energy level of the intermediate node will drop in a much lesser number than that of the existing scheme.

Simulation Time	Without credits	With credits
12000	99400	99400
14000	99300	99300
16000	99250	99250
18000	99250	99250
20000	99250	99200
22000	99200	99200
24000	98650	99200
26000	98650	99100
28000	98550	99100
30000	98550	99050
32000	98550	99050
34000	98550	98950
36000	98550	98950

Table.2 Comparisionof Simulation Time and With and Without Credits.

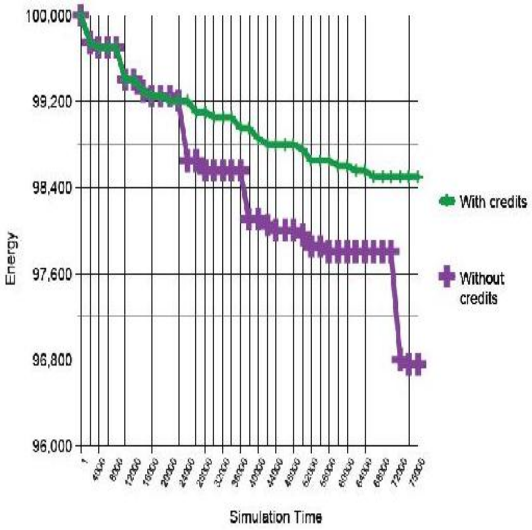


Figure.6 Energy of a Node at Specified Time Interval.

IV. CONCLUSION AND FUTURE WORK

In RACE, a report-based payment scheme for MWNs the nodes submit lightweight payment reports containing the alleged charges and rewards (without proofs), and temporarily store undeniable security tokens called Evidences. The fair reports can be cleared with almost no cryptographic operations or processing overhead, and Evidences are submitted and processed only in case of cheating reports inorder to identify the cheating nodes. Our analytical and simulation results demonstrate that this model effectively identifies attacks like message flooding, packet dropping and ensures that network performance is not compromised. Moreover, RACE can identify the cheating nodes precisely and rapidly without false accusations or missed detections. In RACE, the AC can process the reports to know the number of relayed/dropped messages by each node.

In the future work, a trust system can be developed based on processing the payment reports to maintain a trust value for each node. The nodes that relay messages more successfully will have higher trust values, Based on these trust values, a trust-based routing protocol can be proposed to route messages through the highly trusted nodes to minimize the probability of dropping the messages, and thus improve the network performance in terms of throughput and packet delivery ratio.

REFERENCES

[1] G. Shen, J. Liu, D. Wang, J. Wang, and S. Jin, "Multi-Hop Relay for Next-Generation Wireless Access Networks," Bell Labs Technical J.,vol. 13, no. 4, pp. 175-193, 2009.

[2] C. Chou, D. Wei, C. Kuo, and K. Naik, "An Efficient Anonymous Communication Protocol for Peer-to-Peer Applications Over Mobile Ad-Hoc Networks," IEEE J. Selected Areas in Comm.,vol. 25, no. 1, pp. 192-203, Jan. 2007.

[3] H. Gharavi, "Multichannel Mobile Ad Hoc Links for Multimedia Communications," Proc. IEEE, vol. 96, no. 1, pp. 77-96, Jan. 2008.

[4] S. Marti, T. Giuli, K. Lai, and M. Baker, "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks," Proc. MobiCom '00,pp. 255-265, Aug. 2000.

[5] G. Marias, P. Georgiadis, D. Flitzanis, and K. Mandalas,"Cooperation Enforcement Schemes for MANETs: A Survey,"Wiley's J. Wireless Comm. and Mobile Computing, vol. 6, no. 3,pp. 319-332, 2006.

[6] L. Buttyan and J. Hubaux, "Stimulating Cooperation in SelfOrganizing Mobile Ad Hoc Networks," Mobile Networks and Applications, vol. 8, no. 5, pp. 579-592, Oct. 2004.

[7] Y. Zhang, W. Lou, and Y. Fang, "A Secure Incentive Protocol for Mobile Ad Hoc Networks," ACM Wireless Networks, vol. 13, no. 5,pp. 569-582, Oct. 2007.

[8] A. Weyland, "Cooperation and Accounting in Multi-Hop Cellular Networks," PhD thesis, Univ. of Bern, Nov. 2005.

[9] A. Weyland, T. Staub, and T. Braun, "Comparison of MotivationBased Cooperation Mechanisms for Hybrid Wireless Networks,"J. Computer Comm., vol. 29, pp. 2661-2670, 2006.