ISSN No. 0976-5697

Volume 3, No. 1, Jan-Feb 2012

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

A Special Acknowledgement based Routing for Mesh Network

B. Raj Kumar
Assoc. Professor in CSE Dept
S.R. Engineering College
Ananthasagar, Warangal, India
raj_kumar_b@srecwarangal.ac.in

G. Aruna Kranthi
Sr. Asst. Professor in CSE Dept
S.R. Engineering College
Ananthasagar, Warangal, India
raj.kranthi@gmail.com

Bhandari Phaniraja*
Computer Science and Engineering
S.R. Engineering College
Ananthasagar, Warangal, India
phaniraja8@gmail.com

Abstract: Within the last few years, prevalence and importance of wireless networks increased significantly. Especially, wireless mesh networks received a lot of attention in both academic research and commercial deployment. The networking performance of the mesh can degraded gradually, if a node gets malicious. Internal malicious nodes are the prime reason of most of the attacks in network and only few works have done in preventing the internal nodes which are compromised from degrading the performance. In this paper, we propose the Special Acknowledgment (SpAck) scheme that can be put as an optional feature for HWMP to detect node misbehavior and to find out malicious node. The main technique of the SpAck scheme is to forward Special acknowledgment packets. The effectiveness of SpAck based HWMP is analyzed through simulation

Keywords: Trust; Reactive Routing; Security; HWMP; Mesh.

I. INTRODUCTION

Wireless Mesh Networks are defined by mesh nodes which provide a distributed infrastructure for mobile client node. The wireless mesh network has many applications and uses. Its features include low cost, easy establishment and maintenance. Wireless Mesh networks have gateway nodes which are used to connect external network and mesh nodes are used to connect internal mobile clients. Hybrid Wireless Mesh Networks is being developed as a routing protocol for IEEE 802.11s WLAN Mesh Networking, the different modes of hybrid wireless mesh Protocol works well with different environments [1]. Reactive mode is good for small root traffic whereas proactive mode has good packet delivery ratio and path optimality for increasing root traffic [1].

IEEE 802.11s does not specify much about security in HWMP, but secure version of HWMP uses existing key hierarchy, where symmetric encryption is used for non-mutable field and uses merkle tree technique to authenticate mutable field [2]. There may exist a malicious node which being compromised by an attacker has access to all the key and authentication information, which may perform attacks such as pin attack, flooding, location disclosure, energy exhaustion and loops [3]. So new and advanced Security techniques are needed to defend internal malicious node's attacks and threats, trust is an important aspect which may provide mechanism to defend such attacks. A trust based model defines, evaluates and links up trust based relationships among stations. A trust system can track the behavior of nodes and thereby proceed by detecting and punishing misbehaving ones.

In our framework mesh nodes interact only with its neighbors. As a result, nodes do not store trust information about every node in the network. Storing neighborhood information defines significant lower energy consumption, less processing for trust level calculation, and less memory space.

In This paper, we proposes a trust based security solutions, trust evaluation based model can provide security using factors such as experience statistics, special acknowledgment, routing request, etc. and it embroils developing a trust based model, defining credits to nodes, maintaining the trust value of each node, and evaluating proper decisions about nodes maliciousness.

The remainder of the paper is structured as follows: Section II deals with related Work. The proposed Trust based Framework is discussed in Section III, Section IV describes the extensions to the network simulator ns-3 that had to be implemented in order to allow for simulation of wireless mesh networks and simulation results are presented and discussed. Finally, Section V describes related work before Section VI gives a conclusion and future work.

II. RELATED WORK

Trust is a certain level of the subjective probability with which a node will achieve a particular deed, both before we can observe such a deed and in a context in which it marks our own deed. Developing a secured system using trust based mechanisms is quite an interesting approach and several techniques as described in the following subsection that can be applied to a distributed application environment like a WMN.

The distributed trust model proposed in [4] makes use of a decentralized approach to manage trust and a recommendation protocol to exchange trust related information. The model is based on a conditional transitive trust relation that uses trust categories to express trust towards other agents. In order to establish trust relation between entities where a direct relation does not exist, the agents can make use of an intermediate agent to establish trust. The trust techniques can be roughly classified into three schemes: reputation-based schemes, credit-based schemes, and Acknowledgment based schemes.

A. Reputation-based schemes:

a. Watchdog and Pathraters:

The Watchdog and Pathrater mechanism [8] has been defined to optimize and increase the forwarding mechanism in the DSR protocol. The mechanism basically consists of two parts: Watchdog and Pathrater. The Watchdog is used to detect selfish nodes that do not forward packets. The Pathrater assigns evaluation to the nodes based upon the response that it receives from the Watchdog. Then routes are selected depending upon the evaluations, generally consisting of nodes with the highest forwarding rate. During route selection, these evaluated rates are averaged over all nodes that are present in a path and the path with the best evaluated rate is accepted.

b. Core:

CORE (COllaborative REputation) defines a reputation based exchange mechanism. CORE divides the status of a node into three components: Functional Reputation is defined upon behavior evaluated during a specific task. Positive trust ratings are replaced and the negative ratings are locally resultant by the Watchdog. Subjective Reputation defines its own observations and Indirect Reputation, defined by the report given by other node.

c. Confidant:

CONFIDANT (Cooperation Of Nodes, Fairness In Dynamic ad hoc NeTworks) [9] defines a trust based manager and a reputation system to the Watchdog and Pathrater scheme. The warning of malicious node is issued, whenever the trust based manager evaluates the events reported by the monitor. A user-to-user authentication mechanism [10] is used to maintain a friend list which is used to maintain the alarm recipient's. Whenever the trust level drops below a certain threshold, then the CONFIDANT protocol will not forward the packets to that node.

B. Acknowledgment based schemes:

To detect routing misbehavior or malicious nodes in wireless networks, there are several schemes that use end-to-end acknowledgments (ACKs). In Acknowledgement based approach [7], they use 2Ack scheme that is to send a two-hop acknowledgment packets in the opposite direction of the routing path to detect the malicious node. Only a fraction of the data packets received are acknowledged in the 2ACK scheme, to reduce routing overhead

C. Currency-Based Schemes:

The TermiNodes project [5], [6] uses a currency called nuglets, which is used as a payment per forwarded packet. The nuglets are upheld by each node in a secure way. There is no way of misuse of nuglets, because of cryptographic infrastructure which is used to ensure accuracy in transactions. With every forwarded packet, there will be an increase in the number of nuglets and decrease with each originated packet. There are two charging models: Packet trade model (Recipient to pay) and Packet purse model (Sender to pay).

III. THE SPACK SCHEME

Every hop link will have sender and receiver which can be malicious. We concentrate on the problem of detecting links which are misbehaving instead of nodes. A misbehaving node which might be a sender or a receiver of hop link will not forward the data packet further. That link will be tagged. Our scheme discussed her simplifies the link detection mechanism.

A. Details of the SpAck Scheme:

To detect misbehaving links and to mitigate their effects, we use special acknowledgement scheme at a MAC-layer. It is employed as an optional-technique to existing routing protocols for Mesh, such as HWMP. We use of a new type of acknowledgment packet, called SpAck to detect misbehavior. Suppose that A, B, and C are three sequential nodes in a route. In the Route Request phase of the HWMP protocol, a route is generated from source node, S, to a destination nod. Whenever A sends a data packet to B, it is not clear for A, that B has sent the data packet or not. Such vagueness exists even when there are no misbehaving nodes. There might be potential misbehaving nodes in an open mesh network which may increase the severity of a problem.

Node C would send an explicit acknowledge to A on its successful reception of a data packet. It would send out a SpAck packet over two hops to A with the ID of the corresponding data packet, whenever node C receives the data packet successfully. The SpAck packet receiver or the observing node (i.e. node A) and C as SpAck packet sender is used in further discussion. Every set of Triplets (A-B-C) along the route takes place a SpAck transmission and therefore, SpAck packet sender only cannot be the first router from the source. SpAck receivers cannot be the last router just before the destination and the destination.

The SpAck packet sender maintains a list of IDs of data packets that have not been acknowledged, to detect misbehavior. Suppose S sends a data packet on a path, say, An in Figure 1, which consist of LIST which illustrates the data structure maintained by the observing node. Whenever data packet is forwarded, Cpkts is incremented. At A, each packet ID will be on the list for t time, which is used as a timeout. The ID will be removed from the list whenever a SpAck packet corresponding to this ID arrives. Otherwise, Cmis will be incremented and the ID will be removed at the end of its timeout interval. A SpAck packet (refer to Figure 2) to A is sent Whenever C receives appropriate data packet.

B Next Hop Receiver	C Second Hop Receiver	Cpkts: Packets Transmitted	Cmiss: SpAck Packets Missed	List: List of Data packet IDs

Figure 1.Data structure maintained by the observing node

Rack is termed as fraction of acknowledgment ratio and it is used to reduce the additional routing overhead caused by the SpAck scheme, only a Rack fraction of the data packets will be acknowledged. By changing Rack, we can adjust the overhead of SpAck packet transmissions. Router A calculates the ratio of missing SpAck packets and compares it with a threshold Rmis. If the ratio is greater than Rmis, hop link B-C is declared as misbehaving. Since only a Rack of the received data packets are acknowledged. Rmis should fulfill Rmis > 1 - Rack in order to eradicate incorrect alarms caused by such an incomplete acknowledgment mechanism. Such misbehaving links are avoided as a part of its route, whenever a node starts its own data traffic

Table 1.The format of SpAck Report

Ttl(2)	PacketCount	SpAck Sender Address	SpAck Receiver Address	Packet Id received

IV. SIMULATION ENVIRONMENT AND RESULTS

We use Network Simulator 3 [11], which is an actively developed discrete-event network simulator used for research and educational use.

A. Mesh module:

The UML diagram of mesh module [12] core class is shown on Figure 2. It is 2 tier architecture: the station tier includes mesh point device and mesh protocols, while the interface tier includes mesh interfaces and protocols plugins {a concept to be defined below. The mesh station is modeled with special kind of network device, class MeshPointDevice, with routing functionality and control over underlying real network devices (interfaces) hidden from the upper-layer protocols, class WifiNetDevice.

This network device operates by the following scheme: it receives a packet, makes all route discovery procedures, chooses an output interface and sends a packet. When receiving a packet, it delivers a packet to upper-layer protocols or forwards it further to a proper interface using routing protocol. Note, that any other network devices can coexist with MeshPointDevice on the same node. Every MeshPointDevice has its own MAC address, known by network layer protocols. It is asserted, that single interface MeshPointDevice has an address of its interface. MAC addresses of the individual mesh interfaces are hidden from upper layers. Apart of being the coordinator of its interfaces, mesh point device serves as the fixing point of all mesh protocols. The examples of mesh protocols are Peering Management Protocol and HWMP, discussed above.

B. Simulation Environment:

There are two Scenarios, which are static grids of 9 (3 x 3) mesh stations; each station can communicate with maximum 4 neighbors by the grid cell sides.

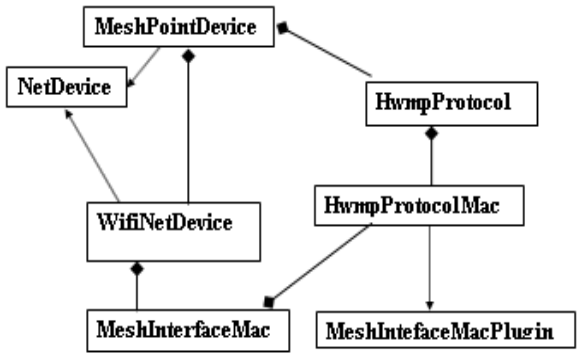

Figure 2.Mesh Module's in Ns3.

a. Addressing:

802.11s mesh stations are addressed using unique 48-bitMAC addresses. If mesh station has multiple physical interfaces then both station and every interface is addressed, it is assumed that station itself has an address of its first interface. The minimal information needed for successful multi-hop frame delivery includes four addresses: two of them being the frame original source and final destination and another two are current transmitter and receiver. This is known as 4-address addressing scheme. To forward frames, originating or ending (or both) at a point outside of mesh network, one or two additional addresses are required. This is known as 6-address scheme. Additional, comparing to standard 802.11 headers, addresses are placed in the dedicated 6 to 24 octets long Mesh Control header which is added to all multi-hop frames right before 802.11 headers.

b. Link metrics:

HWMP is defined for operation with arbitrary path link metrics, e. g. hop count or radio-aware metrics—the latter consider not only the topology but also the condition of the wireless transmission medium. The IEEE 802.11s draft standard e. g. specifies the airtime link metric as a radio-aware metric.

c. Evaluation scenarios:

There are two scenarios as follow

a. Default scenario with single Malicious node

One of the nodes will be considered as a malicious node, which drops the data packets at rate of **Rpart** after participating in the route formation. This forms a packet loss in the scenario.

b. Trusted HWMP with single Malicious node

By using this trusted framework, the nodes in the network can detect the malicious node and it shows the route will not be initiated from that node in next iterations.in such way that misbehaving node will not be able to send data in the network.

d. Evaluation metrics:

There are two Evaluation Metrics as follow

a. Packet Delivery Ratio (PDR): It is the ratio of data packets being successfully received by the destination

mesh stations versus data packets being sent by the source mesh stations.

b. Malicious Node Detection

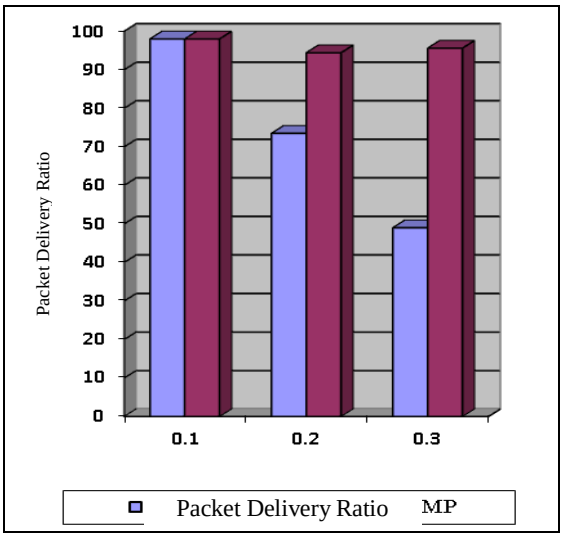

Figure 3.PDR over Rpart

C. Simulation results:

a. Packet delivery ratio:

As shown in the figure, the difference between the default scenario and trusted scenario is huge and it depends upon the Rpart rate at which data packets being dropped by the malicious node. When Rpart is 0.1, In Which the Malicious node drop the 1 of 10 data packets received. So SpAck Scheme cannot detect malicious node because, it Assumes it may occurred due network congestion or collision, etc. but when the Rpart is above 0.2, then SpAck Scheme would decrease the trust value, due to which the route would change and node will declared as a malicious if it degrades below the threshold. We can also see the way the trust values are acting on the malicious node with different Rpart rate.

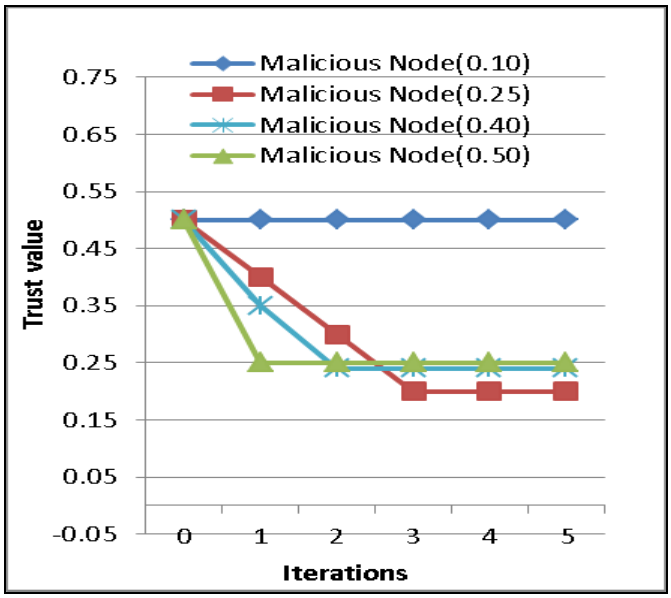

Figure 4.Trust values Of Malicious Node

b. Malicious Node Detection

As shown in the figure 5, the default route is 9-6-3-2-1, where source node is 9 and destination node is 1. We choose 3 as malicious node and changed the Rpart to 0.5, so that it will drop the data packets at 5 of 10 packets received, which will decrease its trust value less than threshold. So In next iterations, the misbehaving node will not be able to take part in Route Discovery Process, as shown in the figure

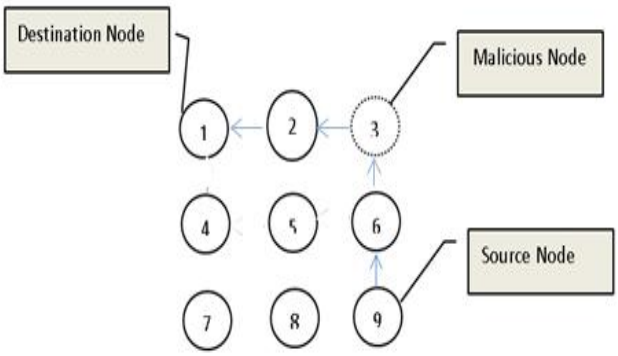

Figure 5.Route By HWMP

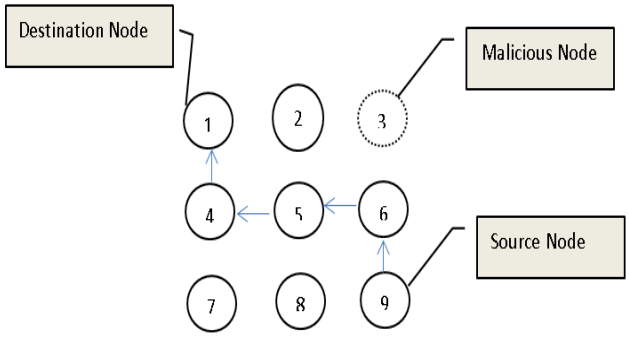

Figure 6.Route By SpAck HWMP

V. CONCLUSION AND FUTURE WORK

Mesh networks is dependent on the collaboration of all of its nodes to perform networking tasks. Mischievous Nodes can degrade the performance of the network and routing is one such area, which is vulnerable to such nodes. Routing performance may be degraded severely, whenever such misbehaving nodes refuse to forward the data packets, even though participating in the Route Discovery phase.

In this paper, we have proposed SpAck scheme and evaluated it, to identify and alleviate the effect of such routing misbehavior. The SpAck scheme is based on sender receiving a special 2-hop acknowledgment packet that is sent back by the receiver of the hop link. Compared with other approaches to combat the problem, such as the overhearing technique, the SpAck scheme overcomes several problems including receiver collisions, limited transmission powers and ambiguous collision. The SpAck technique can be used as an optional method to HWMP in Mesh Networks. The detailed presentation of SpAck scheme is presented. We have studied that SpAck scheme upholds up to 92 percent of PDR even

when there is 50 percent of data packet drop ratio in misbehaving node in the Mesh Networks using simulations.

The default HWMP scheme can only offer a packet delivery ratio of 50 percent. The SpAck scheme has the flexibility to control overhead with the use of the Rack parameter which its advantage. To specifically detect a misbehaving node, we have to check the behavior of links around that node. This is our future work. Theoretical analysis of the performance increase of the SpAck scheme is also of interest.

VI. REFERENCES

[1] Malte Cornils, Michael Bahr and Thomas Gamer, "Simulative Analysis of the Hybrid Wireless Mesh Protocol (HWMP)", 2010 European Wireless conference.

[2] Md. Shariful Islam, Young Jig Yoon, Md. Abdul Hamid, and Choong Seon, "A Secure Hybrid Wireless Mesh Protocol for 802.11s Mesh Network", ICCSA 2008, Part I, LNCS 5072, pp. 972–985, 2008.

[3] Anil Kumar Gankotiya1, Sahil Seth2, Gurdit Singh3,"Attacks and their Counter Measures in Wireless Mesh Networks", Cyber Security Research Center

[4] Abdul-Rahman Alfarez, Halles Stephen,A Distributed Trust Model, In Proc. Of New Security Paradigms Workshop, ACM, New York, NY, USA, 1998..

[5] L. Buttyan and J. Hubaux, "Enforcing Service Availability in Mobile Ad Hoc WANs," Proc. IEEE/ACM Workshop Mobile Ad Hoc Networking and Computing (MobiHOC), pp. 87-96, 2000.

[6] L. Buttyan and J. Hubaux, "Stimulating Cooperation in Self-Organizing Mobile Ad Hoc Networks," Proc. ACM/Kluwer Mobile Networks and Applications (MONET), vol. 8, pp. 579-592, 2003.

[7] Kejun Liu, Jing Deng, Pramod K. Varshney, Kashyap Balakrishnan, An Acknowledgment-Based Approach for the Detection of Routing Misbehavior in MANETs,In Proc IEEE TRANSACTIONS ON MOBILE COMPUTING, MAY 2007

[8] A.A. Pirzada, A. Datta, and C. McDonald, "Trust Based Routing for Ad Hoc Wireless Networks," Proc. IEEE Int'l Conf. Networks (ICON '04), pp. 326-330 2004.

[9] S. Marti, T. Giuli, K. Lai, and M. Baker, "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks," Proc. Sixth Ann. Int'l Conf. Mobile Computing and Networking (MobiCom), pp. 255-265,2000.

[10] S. Buchegger and J. Boudec, "Performance Analysis of the CONFIDANT Protocol: Cooperation of Nodes—Fairness in Distributed Ad Hoc NeTworks," Proc. IEEE/ACM Workshop Mobile Ad Hoc Networking and Computing (MobiHOC), pp. 226-236, 2002.

[11] The ns-3 network simulator. http://www.nsnam.org/.

[12] Kirill Andreev, Pavel Boyko, E 802.11s Mesh Networking NS-3 Model".