Detection of Routing Misbehavior in MANETs with 2ACK scheme

Chinmaya Kumar Nayak[1], G K Abani Kumar Dash[2], Kharabela parida[3] and Satyabrata Das [4]
[1,2,3,4] Department of Computer Science and Engineering, College of Engineering Bhubaneswar,
BPUT, Odisha, INDIA
[1]Chinmaya.confidentone@gmail.com, [2]abanidash1982@gmail.com, [3]kharabelaparida@gmail.com,
[4]satya.das73@gmail.com

***Abstract*—The Routing misbehavior in MANETs (Mobile Ad Hoc Networks) is considered in this paper. Commonly routing protocols for MANETs [1] are designed based on the assumption that all participating nodes are fully cooperative. Routing protocols for MANETs are based on the assumption which are, all participating nodes are fully cooperative. Node misbehaviors may take place, due to the open structure and scarcely available battery-based energy. One such routing misbehavior is that some nodes will take part in the route discovery and maintenance processes but refuse to forward data packets. In this, we propose the 2ACK [2] scheme that serves as an add-on technique for routing schemes to detect routing misbehavior and to mitigate their effect. The basic idea of the 2ACK scheme is to send two-hop acknowledgment packets in the opposite direction of the routing path. To reduce extra routing overhead, only a few of the received data packets are acknowledged in the 2ACK scheme.**

Keywords- MANET; routing in MANETS; misbehavior of nodes in MANETS; credit based scheme; reputation based scheme; the 2ACK scheme; network security.

I. INTRODUCTION

A. MOBILE ADHOC NETWORK

Mobile Ad-hoc networks (MANET) are self-configuring and self-organizing multi hop wireless networks where, the network structure changes dynamically. In a MANET nodes (hosts) communicate with each other via wireless links either directly or relying on other nodes as routers [3]. The nodes in the network not only acts as hosts but also as routers that route data to/from other nodes in network The operation of MANETs does not depend on preexisting infrastructure or base stations. Network nodes in MANETs can move freely and randomly.

An Example is shown in figure 1. Node A can communicate directly (single hop) [4] with node C, node D and node B. If A wants to communicate with node E, node C must work as an intermediate node for communication between them. That's why the communication between nodes A and E is multi-hop. The operation of MANETs does not depend on preexisting infrastructure or base stations. Network nodes in MANETs can move freely and randomly.

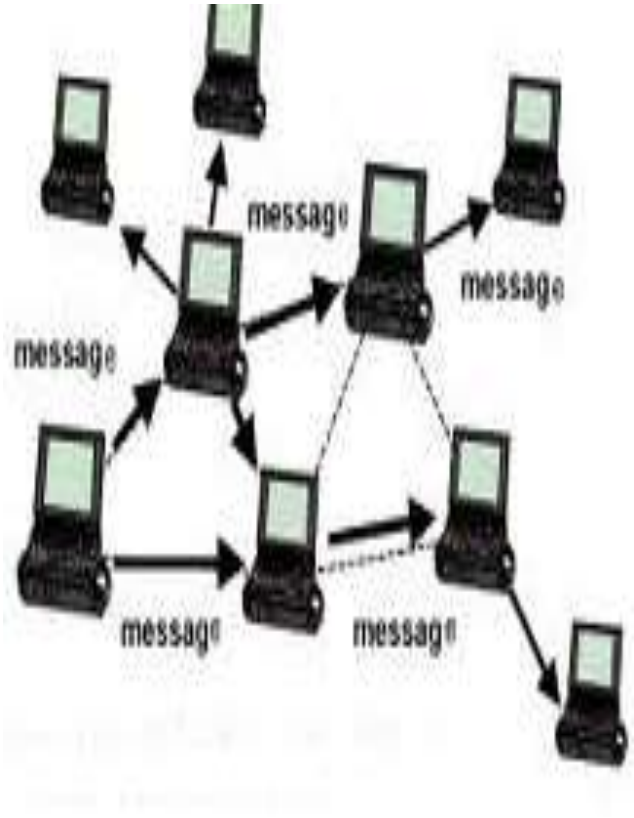

Figure 1: A Mobile ad hoc network

B. CHARACTERSTICS OF MANETS:

- It having the dynamic topology, which links formed and broken with mobility.
- Possibly uni-directional links [4].
- Constrained resources like battery power and wireless transmitter range.
- Network partitions.

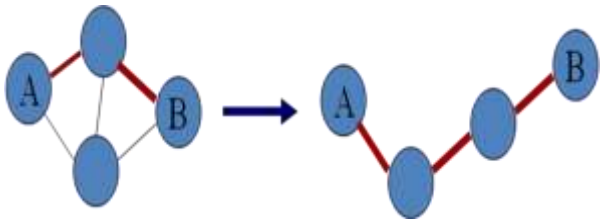

Figure 2: Representation of dynamic topology

C. MANET ROUTING

To find and maintain routes between dynamic topology with possibly uni-directional links, using minimum resources. The use of conventional routing protocols in a dynamic network is not possible because they place a heavy burden on mobile computers and they present convergence characteristics that do not suit well enough the needs of dynamic networks [5]. For Example, any routing scheme in a dynamic environment for instance ad hoc networks must consider that the topology of the network can change while the packet is being routed and that the quality of wireless links is highly variable. The network structure is mostly static in wired networks that are why link failure is not frequent. Therefore, routes in MANET must be calculated much more frequently in order to have the same response level of wired networks. Routing schemes in MANET are classified in four major groups, namely, proactive routing, flooding, reactive routing, and hybrid routing [6].

D. MISBEHAVIOUR OF NODES IN MANET:

Ad hoc networks increase total network throughput by using all available nodes for forwarding and routing. Therefore, the more nodes that take part in packet routing, the greater is the overall bandwidth, the shorter is the routing paths, and the smaller the possibility of a network partition. But, a node may misbehave by agreeing to forward packets and then failing to do so, because it is selfish, overloaded, broken, or malicious [7].

An overloaded node lacks the buffer space, CPU cycles or available network bandwidth to forward packets. A selfish node is unwilling to spend CPU cycles, battery life or available network bandwidth to forward packets not of direct interest to it, even though it expects others to forward packets on its behalf. A malicious node creates a denial of service (DOS) [7] attack by dropping packets. A broken node might have a software problem which prevents it from forwarding packets.

II. PROPOSED MODEL

A. THE 2ACK SCHEME

The main idea of the 2ACK scheme is to send two-hop acknowledgment packets in the opposite direction of the routing path. In order to reduce additional routing overhead, only a fraction of the received data packets are acknowledged in the 2ACK scheme. Thus it detects the misbehaving nodes, eliminate them and choose the other path for transmitting the data. The watchdog detection mechanism has a very low overhead. Unfortunately, the watchdog technique suffers from several problems such as ambiguous collisions, receiver collisions, and limited transmission power [8]. The main issue is that the event of successful packet reception can only be accurately determined at the receiver of the next-hop link, but the watchdog technique only monitors the transmission from the sender of the next-hop link.

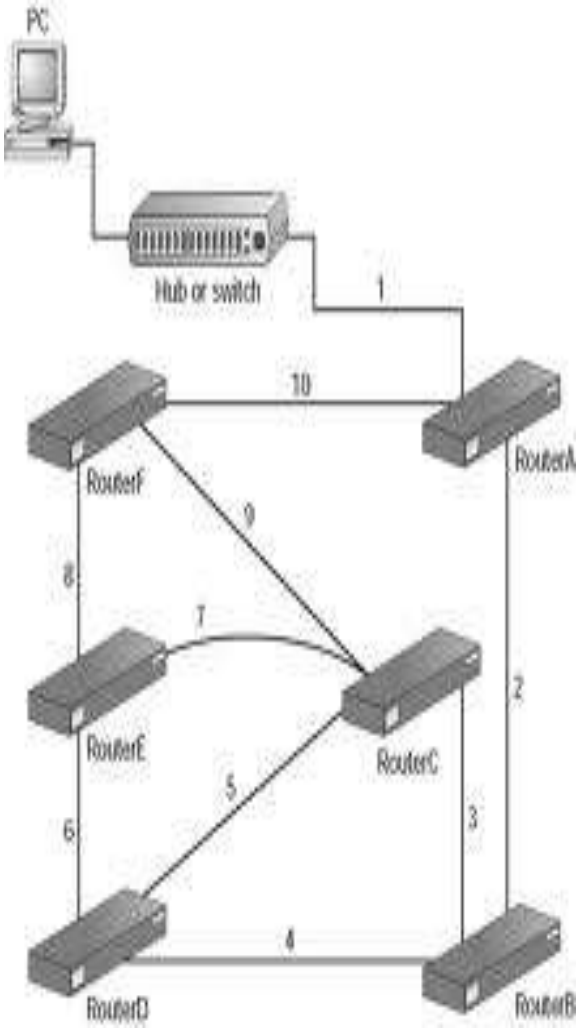

Figure 3: Scenario for packet dropping and misrouting

Noting that a misbehaving node can either be the sender or the receiver of the next-hop link, we focus on the problem of detecting misbehaving links instead of misbehaving nodes. In the next-hop link, a misbehaving sender or a misbehaving receiver has a similar adverse effect on the data packet [8]: It will not be forwarded further. The result is that this link will be tagged. 2ACK scheme significantly simplifies the detection mechanism.

B. DETAILS OF THE 2ACK SCHEME

The 2ACK scheme is a network-layer technique to detect misbehaving links and to mitigate their effects. It can be implemented as an add-on to existing routing protocols for MANETs, such as DSR. The 2ACK scheme detects misbehavior through the use of a new type of acknowledgment packet, termed 2ACK. A 2ACK packet is assigned a fixed route of two hops (three nodes) in the opposite direction of the data traffic route.

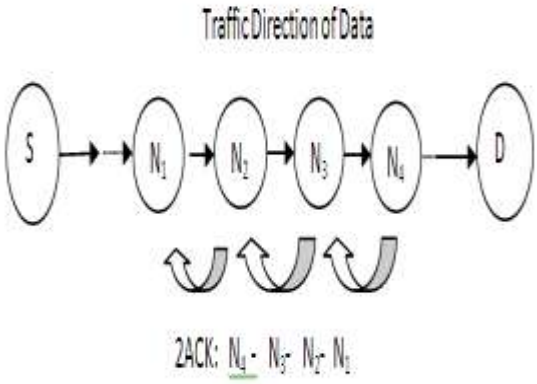

Figure 4: The 2ACK Scheme

Figure 4 illustrates the operation of the 2ACK scheme. Suppose that N1, N2, N3 and N4 are three consecutive nodes (tetra) along a route [9]. The route from a source node, S, to a destination node, D, is generated in the Route Discovery phase of the DSR protocol. When N1 sends a data packet to N2 and N2 forwards it to N3 and so on, it is unclear to N1 whether N3 or N4 receives the data packet successfully or not. Such an ambiguity exists even when there are no misbehaving nodes. The problem becomes much more severe in open MANETs with potential misbehaving nodes.

The 2ACK scheme requires an explicit acknowledgment to be sent by N3 and N4 to notify N1 of its successful reception of a data packet: When node N3 receives the data packet successfully, it sends out a 2ACK packet over two hops to N1 (i.e., the opposite direction of the routing path as shown), with the ID of the corresponding data packet. The triplet N1 → N2 → N3→ N4 is derived from the route of the original data traffic.

Such a tetra is used by N1 to monitor the link N2 →N3→ N4. For convenience of presentation, we term N1 in the tetra N1 → N2 → N3→ N4 the 2ACK packet receiver or the observing node and N4 the 2ACK packet sender. Such a 2ACK transmission takes place for every set of tetra along the route. Therefore, only the first router from the source will not serve as a 2ACK packet sender. The last router just before the destination and the destination will not serve as 2ACK receivers.

III. APPLICATION

Ad-hoc networks are suited for use in situations where an infrastructure is unavailable or to deploy one is not cost effective.

A mobile ad-hoc network can also be used to provide crisis management services applications, such as in disaster recovery, where the entire communication infrastructure is destroyed and resorting communication quickly is crucial. By using a mobile ad-hoc network, an infrastructure could be set up in hours instead of weeks, as is required in the case of wired line communication. Another application example of a mobile ad-hoc network is Bluetooth, which is designed to support a personal area network by eliminating the need of wires between various devices, such as printers and personal digital assistants. The famous IEEE 802.11 or Wi-Fi protocol also supports an ad-hoc network system in the absence of a wireless access point [9]. Another application example of a mobile ad-hoc network is Bluetooth, which is designed to support a personal area network by eliminating the need of wires between various devices, such as printers and personal digital assistants [10].

IV. ADVANTAGES

As compared to the watchdog, the 2ACK scheme has the following advantages:

*1) **Flexibility [9]:** One advantage of the 2ACK scheme is its flexibility to Control overhead with the use of the Rack parameter.*

*2) **Reliable data Transmission:** It deals with the reliable transfer of file from source to destination. The file needs to be stored at source for certain amount of time even if it has been transmitted. This will help to resend the file if it gets lost during transmission from source to destination.*

*3) **Reliable route discovery [10]:** Reliable Route Discovery deals with discovering multi-hop route for wireless transmission. Routing in a wireless ad-hoc network is complex. This depends on many factors including finding the routing path, selection of routers, topology, protocol etc.*

*4) **Limited Overhearing Range [10]:** A well-behaved N3 may use low transmission power to send data toward N4. Due to N1's limited overhearing range, it will not overhear the transmission successfully and will thus infer that N2 is misbehaving, causing a false alarm. Both this problem occurs due to the potential asymmetry between the communication links. The 2ACK scheme is not affected by limited overhearing range problem.*

*5) **Limited Transmission Power:** A misbehaving N2 may maneuver its transmission power such that N1 can overhear its transmission but N4 cannot. This problem matches with the Receiver Collisions problem. It becomes a threat only when the distance between N1 and N2 is less than that between N2 and N3 and so on. The 2ACK scheme does not suffer from limited transmission power problem.*

V. CONCLUSION

The proposed system is a simulation of the algorithm that detects misbehaving links in Mobile Ad Hoc Networks. The 2ACK scheme identifies misbehavior in routing by using a new acknowledgment packet, called 2ACK packet. A 2ACK packet is assigned a fixed route of two hops (four nodes N1, N2, N3, N4), in the opposite direction of the data traffic route. The system implements the 2ACK scheme which helps detect misbehavior by a 3 hop acknowledgement. The 2ACK scheme for detecting routing misbehavior is considered to be network-layer technique for mitigating the routing effects.

REFERENCES

[1] J. J. Garcia-Luna-Aceves et all: Source Tree Adaptive Routing (STAR) protocol, draft-ietf-manet-star-00.txt, 1998, IETF Internet Draft.

[2] D. Johnson, D. Maltz, Y.C. Hu, and J. Jetcheva. The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks (DSR) in 10th IEEE International Conference, 27-30 Aug 2002,Year of Publication :2002, ICON **2002**

[3] Kong, P. Zerfos, H. Luo, S. Lu, and L. Zhang, "Providing Robust and Ubiquitous Security Support for Mobile Ad-Hoc Networks," Proc. IEEE Int'l Conf. Network Protocols (ICNP '01), 2001.

[4] L.M. Feeney and M. Nilsson. Investigating the Energy Consumption of a Wireless Network Interface in an Ad Hoc Networking Environment, Proc. IEEE INFOCOM, 2001*:* Twentieth Annual Joint Conference of the IEEE Computer and Communications Societies, Volume 3 (2001), Pages. 1548-1557, Year of Publication: 2007

[5] Elizabeth Royer and C-K Toh: A Review of Current Routing Protocols for Ad-Hoc Mobile Wireless Networks. IEEE Personal Communications Magazine, pages 46-55, April 1999.

[6] Josh Broch , David A. Maltz , David B. Johnson , Yih-Chun Hu , Jorjeta Jetcheva , A performance comparison of multi-hop wireless ad hoc network routing protocols, Proceedings of the 4th annual ACM/IEEE international conference on Mobile computing and networking, p.85-97, October 25-30, 1998, Dallas, Texas, United States [doi>10.1145/288235.288256].

[7] K. Balakrishnan, J. Deng, and P.K. Varshney. TWOACK: Preventing Selfishness in Mobile Ad Hoc Networks , Proc. IEEE Wireless Comm. and Networking Conf. (WCNC '05), Mar. 2005,Volume 4,Pages 2137-2142, IEEE Press 2005,Year of Publication:2005

[8] Charles E. Perkins , Pravin Bhagwat, Highly dynamic Destination-Sequenced Distance-Vector routing (DSDV) for mobile computers, ACM SIGCOMM Computer Communication Review, v.24 n.4, p.234-244, Oct. 1994.

[9] Charles E. Perkins , Elizabeth M. Royer, Ad-hoc On-Demand Distance Vector Routing, Proceedings of the Second IEEE Workshop on Mobile Computer Systems and Applications, p.90, February 25-26, 1999.

[10] David B. Johnson, David A. Maltz: Dynamic Source Routing (DSR) in Ad Hoc Wireless Networks. In Mobile Computing, edited by Tomasz Imielinski and Hank Korth, chapter 5, pages 153-181. Kluwer Academic Publishers, 1996.

AUTHORS PROFILE

Chinmaya Kumar Nayak is a scholar of M.Tech (CSE) at College of Engineering, Biju Pattanaik University, Bhubaneswar, Odisha, INDIA. He is an author of the book Data structure using 'C'. He published many papers in national seminars. His research areas include Image processing, Image transformation techniques, Adhoc-network etc.

G K Abani Kumar Dash is a scholar of M.Tech (CSE) at College of Engineering,Biju Pattanaik University, Bhubaneswar, Odisha, INDIA. His research areas includes Image processing, Adhoc-network etc.

Kharabela Parida is a scholar of M.Tech (CSE) at College of Engineering,Biju Pattanaik University, Bhubaneswar, Odisha, INDIA. His research areas includes Datamining, Adhoc-network etc**.**

Satyabrata Das is as Assistant Professor and Head in the department of Computer Sc. & Engineering, College of Engineering Bhubaneswar (CEB) and He is a research scholar in the department of ICT Under F.M University, Balasore. He received his Masters degree from Siksha 'O' Anusandhan University, Bhubaneswar. His research area includes DSP, Soft Computing, Data Mining, Adhoc-network etc. Many publications are there to his credit in many International and National level journal and proceedings.