INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH & DEVELOPMENT

ISSN 2278 – 0211 (Online)

Detecting of Routing Misbehaving in Hybrid Wireless Networks Used an Acknowledgment Based Approach

R. Kumaresan
PG Scholar, Department of CSE, United Institute of Technology, Tamil Nadu, India
S. Aakasham
PG Scholar, Department of CSE, SVS College of Engineering, Tamil Nadu, India

Abstract:
The succeeding wireless network is Hybrid Wireless Networks. It can provide Quality of Service (QoS) requirements in real time transmission for wireless application. But it stream including critical mission application like military use or emergency recovery. Hybrid wireless networks is unified mobile ad-hoc network (MANET) and wireless infrastructure networks. It inherits invalid reservation and race condition problem in Mobile ad-hoc network (MANET). Whereas open medium and wide distribution of node make vulnerable to malicious attackers in Hybrid wireless networks. How to secure routing in Hybrid wireless networks. In this paper, we propose a Enhanced Adaptive ACKnowledgment (EAACK)-implement a new intrusion-detection system for Hybrid wireless networks. It protect Hybrid wireless networks from attacks that have higher malicious behavior detection rate. Analytical and simulation result based on the real human mobility mode. EAACK can provide high secure performance in terms of Intrusion-detection, overhead, transmission delay.

Keywords: *Hybrid wireless networks, Mobile ad-hoc network (MANET), Enhanced Adaptive Acknowledgment (EAACK)*

1. Introduction

The future development of wireless networks has stimulated numerous wireless applications that have been used in wide areas such as emergency services, education, commerce, military, and entertainment. It improved technology and reduced costs, wireless networks have gained much more preferences over wired networks in the past few decades. Nowadays, people wish to watch videos, play games, watch TV, and make long distance conferencing via wireless mobile devices “on the go.” The widespread use of wireless and mobile devices and the increasing demand for mobile multimedia streaming services are leading to a promising near future where wireless multimedia services (e.g., mobile gaming, online TV, and online conferences) are widely deployed. The emergence and the envisioned future of real time and multimedia applications have stimulated the need of high Quality of Service (QoS) support in wireless and mobile networking environments [5]. The QoS support reduces end-to- end transmission delay and enhances throughput to guarantee the seamless communication between mobile devices and wireless infrastructures.

Hybrid wireless networks have been proven to be a better network structure for the next generation wireless networks [6], [7], [8], [9], and can help to tackle the stringent end-to end QoS requirements of different applications. Hybrid networks synergistically combine infrastructure networks and MANETs to leverage each other. Specifically, infrastructure networks improve the scalability of MANETs, while MANETs automatically establish self-organizing networks, extending the coverage of the infrastructure networks. In a vehicle opportunistic access network (an instance of hybrid networks), people in vehicles need to upload or download videos from remote Internet servers through access points (APs) (i.e., base stations) spreading out in a city. Since it is unlikely that the base stations cover the entire city to maintain sufficiently strong signal everywhere to support an application requiring high link rates, the vehicles themselves can form a MANET to extend the coverage of the base stations, providing continuous network connections.

Mobile Ad hoc NETwork (MANET) is a collection of mobile nodes equipped with both a wireless transmitter and a receiver that communicate with each other via bidirectional wireless links either directly or indirectly. Industrial remote access and control via wireless networks are becoming more and more popular these days [35]. One of the major advantages of wireless networks is its ability to allow data communication between different parties and still maintain their mobility. However, this communication is limited to the range of transmitters. This means that two nodes cannot communicate with each other when the distance between the two nodes is beyond the communication range of their own. MANET solves this problem by allowing intermediate par- ties to relay data transmissions. This is achieved by dividing MANET into two types of networks, namely, single-hop and multihop. In a single-hop network, all nodes within the same radio range communicate directly with each other. On the other hand, in a multihop network,

nodes rely on other intermediate nodes to transmit if the destination node is out of their radio range. In contrary to the traditional wireless network, MANET has a decentralized network infrastructure. MANET does not require a fixed infrastructure; thus, all nodes are free to move randomly [10], [27], [29]. MANET is capable of creating a self-configuring and self-maintaining network without the help of a centralized infrastructure, which is often infeasible in critical mission applications like military conflict or emergency recovery. Minimal configuration and quick deployment make MANET ready to be used in emergency circumstances where an infrastructure is unavailable or unfeasible to install in scenarios like natural or human-induced disasters, military conflicts, and medical emergency situations [19], [30].

Owing to these unique characteristics, Hybrid wireless networks is becoming more and more widely implemented in the industry [14], [28]. However, considering the fact that Hybrid wireless networks is popular among critical mission applications, network security is of vital importance. Unfortunately, the open medium and remote distribution of Hybrid wireless networks make it vulnerable to various types of attacks. For example, due to the nodes' lack of physical protection, malicious attackers can easily capture and compromise nodes to achieve attacks. In particular, considering the fact that most routing protocols in Hybrid wireless networks assume that every node in the network behaves cooperatively with other nodes and presumably not malicious [5], attackers can easily compromise Hybrid wireless networks by inserting malicious or non-cooperative nodes into the network. Furthermore, because of Hybrid wireless networks distributed architecture and changing topology, a traditional centralized monitoring technique is no longer feasible in Hybrid wireless networks. In such case, it is crucial to develop an intrusion-detection system (IDS). specially designed for Hybrid wireless networks. Many research efforts have been devoted to such research topic [1], [3], [6]–[9], [15], [16], [22], [24], [26], [29],[31].

In the next section, we mainly concentrate on discussing the background information required for understanding this research topic

2. Problem Definition

Our proposed approach EAACK is designed to tackle three of the six weaknesses of Watchdog scheme, namely, false misbehavior, limited transmission power, and receiver collision.

In this section, we discuss these three weaknesses in detail.

1. False misbehaviour
2. Limited transmission power
3. Receiver collision

In a typical example of receiver collisions, shown in Fig. 1, after node A sends Packet 1 to node B, it tries to overhear if node B forwarded this packet to node C; meanwhile, node X is forwarding Packet 2 to node C. In such case, node A overhears that node B has successfully forwarded Packet 1 to node C but failed to detect that node C did not receive this packet due to a collision between Packet 1 and Packet 2 at node C.

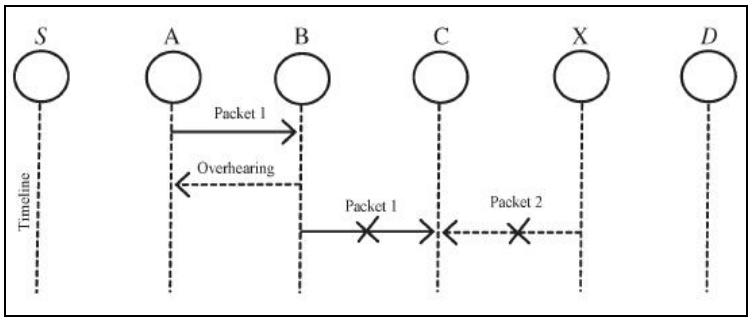

Figure 1: Reveicer collisions

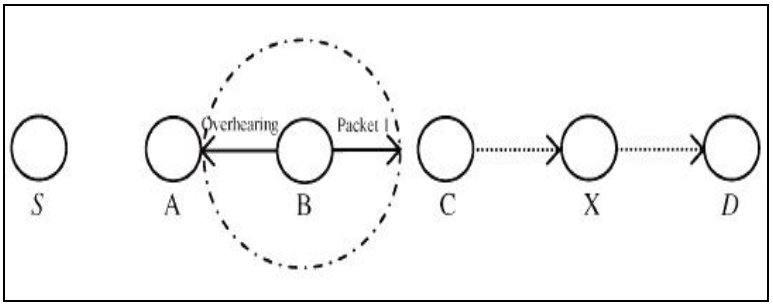

Figure2: Limited Transmission Power

In the case of limited transmission power, in order to preserve its own battery resources, node B intentionally limits its transmission power so that it is strong enough to be overheard by node A but not strong enough to be received by node C, as shown in Fig. 2.

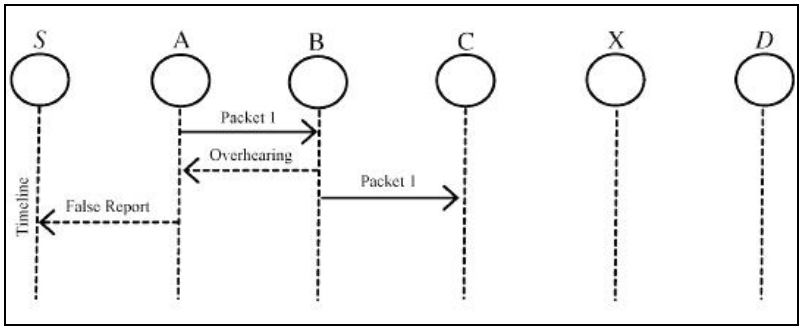

Figure 3: False Misbehavior Report

For false misbehavior report, although node A successfully overheard that node B forwarded Packet 1 to node C, node A still reported node B as misbehaving, as shown in Fig. 3. Due to the open medium and remote distribution of typical MANETs, attackers can easily capture and compromise one or two nodes to achieve this false misbehavior report attack. As discussed in previous sections, TWOACK and AACK solve two of these three weaknesses, namely, receiver collision and limited transmission power. However, both of them are vulnerable to the false misbehavior attack. In this research work, our goal is to propose a new IDS specially designed for MANETs, which solves not only receiver collision and limited transmission power but also the false misbehavior problem.
Furthermore, we extend our research to adopt a digital signature scheme during the packet transmission process. As in all acknowledgment-based IDSs, it is vital to ensure the integrity and authenticity of all acknowledgment packets.

3. Network and Service Models

We consider a hybrid wireless network with an arbitrary number of base stations spreading over the network. N mobile nodes are moving around in network. Each node n_i ($1 \leq i \leq N$) uses IEEE 802.11 interface with the Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) protocol [28]. Since a hybrid network where nodes are equipped with multiinterfaces that transmit packets through multichannels generate much less interference than a hybrid network where nodes are equipped with a single Wi-Fi interface, we assume that each node is equipped with a single Wi-Fi interface in order to deal with a more difficult problem. Therefore, the base stations considered in this paper are access points (APs). The Wi-Fi interface enables nodes to communicate with both APs and mobile nodes. For example, in a University campus, normally only buildings have APs. Therefore, people that do not have Wi-Fi access but close to buildings can use two-hop relay transmissions to connect to the APs in the buildings. Feeney et al. [29] considered the similar scenario in his work.

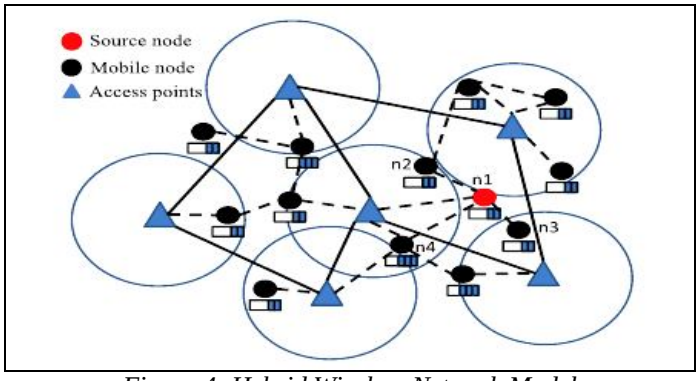

Figure 4: Hybrid Wireless Network Model

The QoS requirements mainly include end-to-end delay bound, which is essential for many applications with stringent real-time requirement. While throughput guarantee is also important, it is automatically guaranteed by bounding the transmission delay for a certain amount of packets [31]. The source node conducts admission control to check whether there are enough resources to satisfy the requirements of QoS of the packet stream. Fig. 4 shows the network model of a hybrid network. For example, when a source node n1 wants to upload files to an Internet server through APs, it can choose to send packets to the APs directly by itself or require its neighbor nodes n2, n3, or n4 to assist the packet transmission.
We assume that queuing occurs only at the output ports of the mobile nodes [32]. After a mobile node generates the packets, it first tries to transmit the packets to its nearby APs that can guarantee the QoS requirements. If it fails (e.g., out of the transmission range of APs or in a hot/dead spot), it relies on its neighbors that can guarantee the QoS requirements for relaying packets to APs. Relaying for a packet stream can be modeled as a process, in which packets from a source node traverse a number of queuing servers to some APs [31]. In this model, the problem of how to secure QoS routing can be transformed to the problem of how to schedule the neighbor resources between nodes to ensure secure QoS of packet routing.

4. Scheme Description

In this paper, we propose a Enhanced Adaptive ACKnowledgment (EAACK).

Specifically, The AODV algorithms used in Hybrid Wireless Networks, if a source node is not within the transmission range of the AP, a source node selects nearby neighbors that can forward its packets to base stations in a distributed manner. The source node schedules the packet streams to neighbors based on their queuing condition, channel condition, and mobility, aiming to reduce transmission time and increase network capacity. The neighbors then forward packets to base stations, which further forward packets to the destination. If any intermediate node cannot send the packets to destination. Check the node if it is affected from any attacker or malicious used Enhanced Adaptive ACKnowledgment (EAACK) scheme.

EAACK is consisted of three major parts, namely, ACK, secure ACK (S-ACK), and misbehavior report authentication (MRA). In order to distinguish different packet types in different schemes, we included a 2-b packet header in EAACK. According to the Internet draft of DSR [42], there is 6 b reserved in the DSR header. In EAACK, we use 2 b of the 6 b to flag different types of packets. Details are described in Table I.

Packet Type	Packet Flag
General Data	00
ACK	01
S-ACK	10
MRA	11

Table 1: Packet Type Indicators

EAACK is consisted of three major parts, namely, ACK, secure ACK (S-ACK), and misbehavior report authentication (MRA). In order to distinguish different packet types in different schemes, we included a 2-b packet header in EAACK. According to the Internet draft of DSR [11], there is 6 b reserved in the DSR header. In EAACK, we use 2 b of the 6 b to flag different types of packets. Details are listed in Table I.

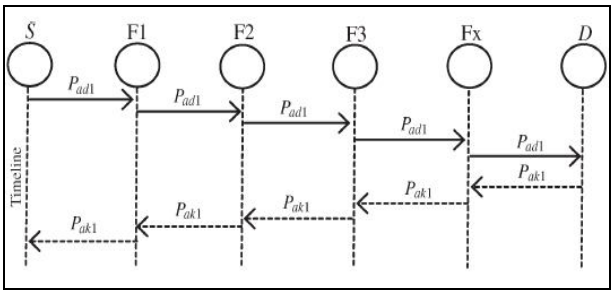

Figure 5: System control flow

Fig. 5 presents a flowchart describing the EAACK scheme. Please note that, in our proposed scheme, we assume that the link between each node in the network is bidirectional. Furthermore, for each communication process, both the source node and the destination node are not malicious. Unless specified, all acknowledgment packets described in this research are required to be digitally signed by its sender and verified by its receiver.

4.1. ACK

ACK is basically an end-to-end acknowledgment scheme. It acts as a part of the hybrid scheme in EAACK, aiming to reduce network overhead when no network misbehavior is detected.

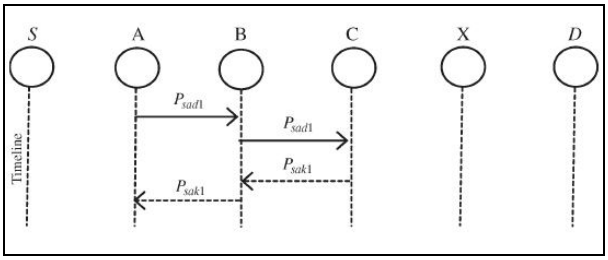

Figure 6: ACK scheme

In Fig. 6, in ACK mode, node S first sends out an ACK data packet $P_{ad}1$to the destination node D. If all the intermediate nodes along the route between nodes S and D are cooperative and node D successfully receives $P_{ad}1$, node D is required to send back an ACK acknowledgment packet $P_{ak}1$ along the same route but in a reverse order. Within a predefined time period, if node S receives $P_{ak}1$, then the packet transmission from node S to node D is successful. Otherwise, node S will switch to S-ACK mode by sending out an S-ACK data packet to detect the misbehaving nodes in the route.

4.2. S-ACK

The S-ACK scheme is an improved version of the TWOACK scheme proposed by Liu *et al.* [44]. The principle is to let every three consecutive nodes work in a group to detect misbehaving nodes. For every three consecutive nodes in the route, the third node is required to send an S-ACK acknowledgment packet to the first node. The intention of introducing S-ACK mode is to detect misbehaving nodes in the presence of receiver collision or limited transmission power. As shown in Fig. 7, in S-ACK mode, the three consecutive nodes (i.e., F1, F2, and F3) work in a group to detect misbehaving nodes in the network. Node F1 first sends out S-ACK data packet $P_{sad}1$ to node F2. Then, node F2 forwards this packet to node F3. When node F3 receives $P_{sad}1$, as it is the third node in this three-node group, node F3 is required to send back an S-ACK acknowledgment packet $P_{sak}1$ to node F2. Node F2 forwards $P_{sak}1$ back to node F1. If node F1 does not receive this acknowledgment packet within a predefined time period, both nodes F2 and F3 are reported as malicious. Moreover, a misbehavior report will be generated by node F1 and sent to the source node S.where the source node immediately trusts the misbehavior report, EAACK requires the source node to switch to MRA mode and confirm this misbehavior report. This is a vital step to detect false misbehavior report in our proposed scheme.

4.3. MRA

The MRA scheme is designed to resolve the weakness of Watchdog when it fails to detect misbehaving nodes with the presence of false misbehavior report. The false misbehavior report can be generated by malicious attackers to falsely report innocent nodes as malicious. This attack can be lethal to the entire network when the attackers break down sufficient nodes and thus cause a network division. The core of MRA scheme is to authenticate whether the destination node has received the reported missing packet through a different route.

To initiate the MRA mode, the source node first searches its local knowledge base and seeks for an alternative route to the destination node. If there is no other that exists, the source node starts a DSR routing request to find another route. Due to the nature of MANETs, it is common to find out multiple routes between two nodes.

By adopting an alternative route to the destination node, we circumvent the misbehavior reporter node. When the destination node receives an MRA packet, it searches its local knowledge base and compares if the reported packet was received. If it is already received, then it is safe to conclude that this is a false misbehavior report and whoever generated this report is marked as malicious. Otherwise, the misbehavior report is trusted and accepted.

By the adoption of MRA scheme, EAACK is capable of detecting malicious nodes despite the existence of false mis-behavior report.

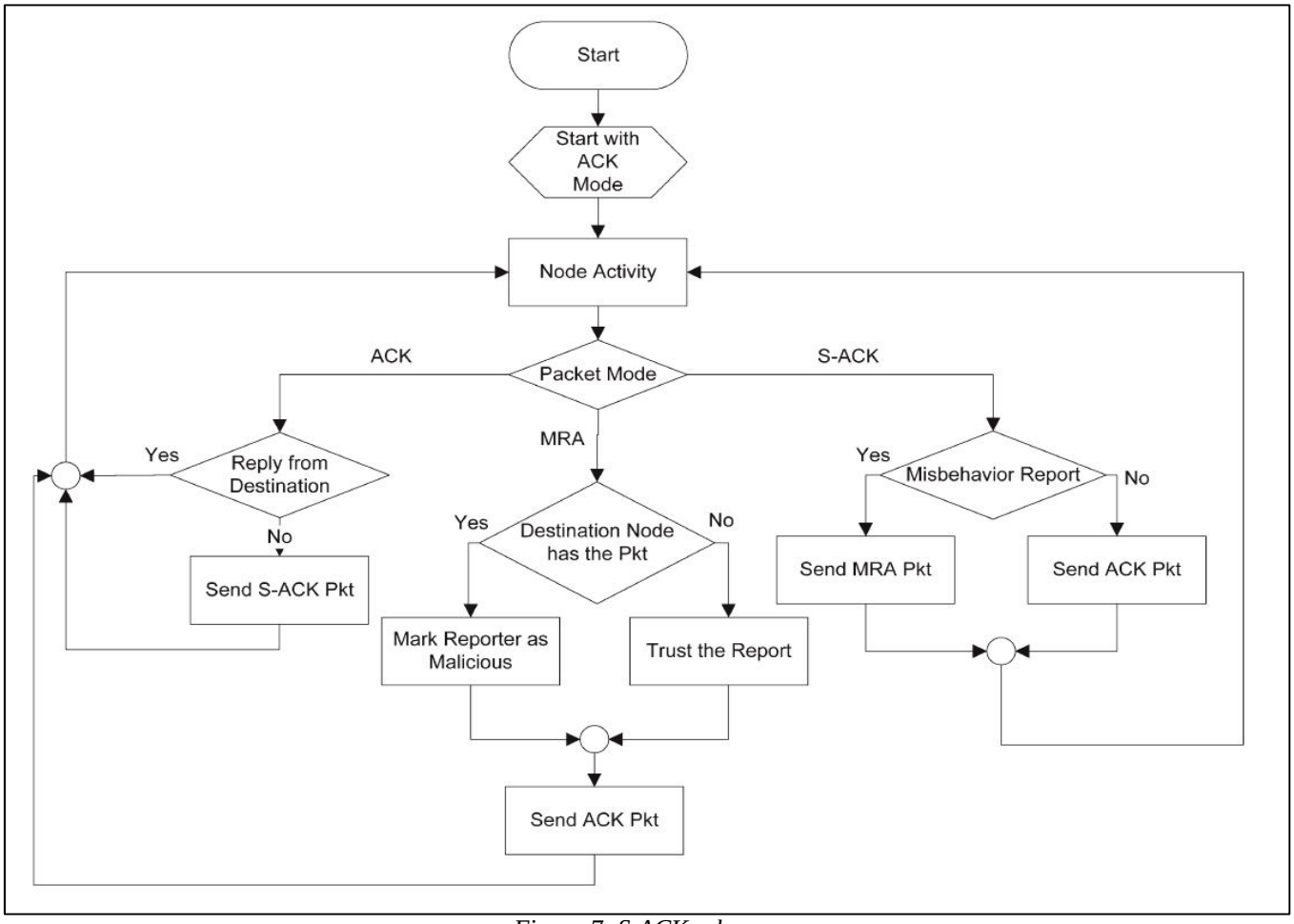

Figure 7: S-ACK scheme

5. Performance Evaluation

This section demonstrates the distinguishing properties of Hybrid Networks compared to MANET through simulations on NS-2 [40]. MANET is a EAACK based routing protocol for Secure routing in MANETs. This protocol extends AODV by adding information of the maximum delay and minimum available bandwidth of each neighbor in a node's routing table. To apply EAACK in hybrid networks, we let a source node search for the secure guaranteed path to an AP. The intermediate nodes along the path reserve the resources for the source node.

In the simulation, the setup was the same as Six APs with IEEE 802.11 MAC protocol are uniformly distributed in the area. We randomly selected two source nodes to send packets to APs in every 10 s. A node's traffic is generated with constant bit rate (CBR) sources. The generation rate of the CBR traffic is 100 kb/s. Unless otherwise specified, the speeds of the nodes were randomly selected from [1-40]m/s. Since the number of successfully delivered packets within a certain delay is critical to the QoS of video streaming applications, we define a new metric, namely QoS guaranteed throughput that measures the throughput sent from a source node to a destination node satisfying a QoS delay requirement as 1 s. This metric can simultaneously reflect delay, packet delivery ratio, throughput, and jitter features of packet transmission.

5.1. Packet Delivery Ratio with Different Mobility Speeds

In this experiment, a node's mobility speed was randomly selected from (1; 10; 20; 30; 40). Fig. 8 plots the packet delivery ratio of all systems versus the node mobility speed. It shows that the packet delivery ratio of all systems decrease as node mobility increases. This is because higher mobility causes higher frequent link breakages, which leads to more packet drops. Reestablishing the broken links results in a long transmission delay for subsequent packets.

In each experiment, during 50 s, we continually selected a certain number of random nodes to transmit packets to their randomly selected destinations for a time period randomly chosen from [1 to 5]s. As the number of source nodes in the system increases, the percentage of the packet delivery ratio increases. This is because as more packets are generated, every packet in the scheduling queue needs to wait for more time to be forwarded out, which leads to higher packet delivery ratio and hence more delivery packets. We also see that the percentage of the packet delivery ration in Hybrid networks is higher than that of MANET.

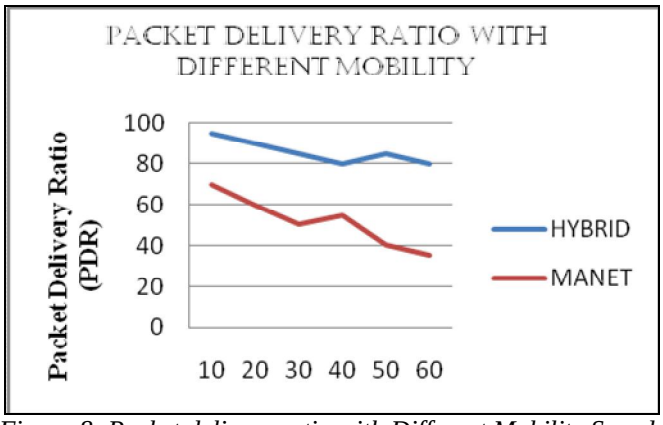

Figure 8: Packet delivery ratio with Different Mobility Speeds

5.2. Delay with Different Mobility Speeds

In this section, we compare Hybrid networks with MANETs for delay. This experiment, a node's mobility speed was randomly selected from (1; 10; 20; 30; 40). Fig. 9 plots the delay of all systems versus the node mobility speed. We let the forwarding nodes receive as many packets from neighbor nodes as possible without admission control to show the performance of Hybrid networks and MANETs when the packets are scheduling infeasible.

In each experiment, during 50 s, we continually selected a certain number of random nodes to transmit packets to their randomly selected destinations for a time period randomly chosen from [1 to 5]s. As the number of source nodes in the system increases, the percentage of the delayed packets increases. This is because as more packets are generated, every packet in the scheduling queue needs to wait for more time to be forwarded out, which leads to higher delay and hence more delayed packets. We also see that the percentage of the delayed packets in MANETs is higher than that of Hybrid networks. This is because EAACK always tries to meet the deadlines of packets with the earliest deadlines, while EAACK tries to balance the delay among the packets. Therefore, EAACK in MANETs is able to meet more deadlines, than it support the QoS routing due to lower queue delay, while EAACK makes full use of the resources of the nodes around a source node, and distributively forwards the packets to the APs, improving the throughput of the system.

.

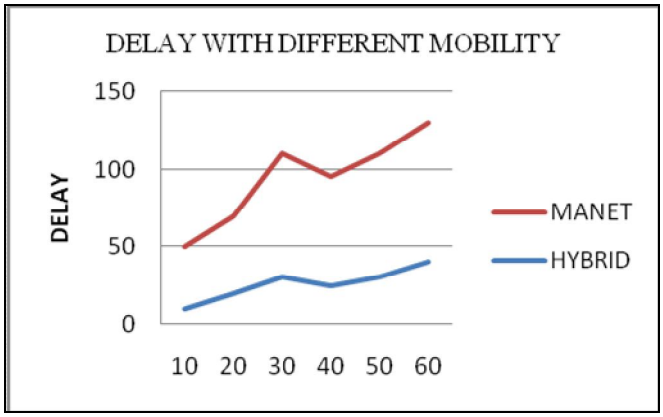

Figure 9: Delay with Different Mobility Speeds

6. Conclusions

Hybrid wireless networks that integrate MANETs and infrastructure wireless networks have proven to be a better network structure for the next generation networks. Packet-dropping attack has always been a major threat to the security in Hybrid wireless networks. In this paper, we propose an Enhanced Adaptive ACKnowledgment (EAACK) for hybrid networks. It provides secure routing services in a highly dynamic scenario. Experimental results show that EAACK can achieve high mobility-resilience, scalability, and contention reduction.

Furthermore, in an effort to prevent the attackers from initiating forged acknowledgment attacks, we extended our research to incorporate digital signature in our proposed scheme. Although it generates more ROs in some cases, as demonstrated in our experiment, it can vastly improve the network's PDR when the attackers are smart enough to forge acknowledgment packets. We think that this tradeoff is worthwhile when network security is the top priority. In the future, we plan to evaluate the performance of EAACK based on the real testbed.

7. References

1. H. Miranda and L. Rodrigues, "Preventing Selfishness in Open Mobile Ad Hoc Networks," Proc. Seventh CaberNet Radicals Workshop, Oct. 2002.
2. L. Buttyan and J.-P. Hubaux, "Security and Cooperation in Wireless Networks," http://secowinet.epfl.ch/, 2006.
3. 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.
4. S. Marti, T. Giuli, K. Lai, and M. Baker, "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks," Proc. MobiCom, Aug. 2000.
5. L. Buttyan and J.-P. Hubaux, "Enforcing Service Availability in Mobile Ad-Hoc WANs," Proc. MobiHoc, Aug. 2000.
6. J.-P. Hubaux, T. Gross, J.-Y. LeBoudec, and M. Vetterli, "Toward Self-Organized Mobile Ad Hoc Networks: The Terminodes Project," IEEE Comm. Magazine, Jan. 2001.
7. S. Buchegger and J.-Y. Le Boudec, "Performance Analysis of the CONFIDANT Protocol: Cooperation of Nodes, Fairness in Dynamic Ad-Hoc Networks," Proc. MobiHoc, June 2002.
8. S. Zhong, J. Chen, and Y.R. Yang, "Sprite: A Simple, Cheat Proof, Credit-Based System for Mobile Ad-Hoc Networks," Proc.
   INFOCOM, Mar.-Apr. 2003.
9. M. Jakobsson, J.-P. Hubaux, and L. Buttyan, "A Micropayment Scheme Encouraging Collaboration in Multi-Hop Cellular Networks," Proc. Financial Cryptography Conf., Jan. 2003.
10. D. Johnson, D. Maltz, Y.C. Hu, and J. Jetcheva, "The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks (DSR)," Internet draft, Feb. 2002.
11. L. Zhou and Z.J. Haas, "Securing Ad Hoc Networks," IEEE Network Magazine, vol. 13, no. 6, Nov./Dec. 1999.
12. F. Stajano and R. Anderson, "The Resurrecting Duckling: Security Issues in Ad-Hoc Wireless Networks," Proc. Seventh Int'l Workshop Security Protocols, 1999.
13. J. 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.
14. I. Aad, J.-P. Hubaux, and E-W. Knightly, "Denial of Service Resilience in Ad Hoc Networks," Proc. MobiCom, 2004.
15. L. Buttyan and J.-P. Hubaux, "Stimulating Cooperation in Self-Organizing Mobile Ad Hoc Networks," ACM/Kluwer Mobile Networks and Applications, vol. 8, no. 5, 2003.
16. V.-N. Padmanabhan and D.-R. Simon, "Secure Traceroute to Detect Faulty or Malicious Routing," SIGCOMM Computer Comm. Rev., vol. 33, no. 1, Jan. 2003.
17. B. Awerbuch, D. Holmer, C.-N. Rotaru, and H. Rubens, "An On- Demand Secure Routing Protocol Resilient to Byzantine Failures," Proc. ACM Workshop Wireless Security (WiSe), Sept. 2002.
18. Y. Xue and K. Nahrstedt, "Providing Fault-Tolerant Ad-Hoc Routing Service in Adversarial Environments," Wireless Personal Comm., vol. 29, nos. 3-4, pp. 367-388, 2004.
19. M. Conti, E. Gregori, and G. Maselli, "Towards Reliable Forwarding for Ad Hoc Networks," Proc. Personal Wireless Comm. (PWC '03), Sept. 2003.
20. Y. Hu, A. Perrig, and D.B. Johnson, "Ariadne: A Secure On- Demand Routing Protocol for Ad Hoc Networks," Proc. MobiCom, Sept. 2002.
21. V. Srinivasan, P. Nuggehalli, C.F. Chiasserini, and R.R. Rao, "Cooperation in Wireless Ad Hoc Networks," Proc. INFOCOM, Mar.-Apr. 2003.
22. R. Mahajan, M. Rodrig, D. Wetherall, and J. Zahorjan, "Sustaining Cooperation in Multi-Hop Wireless Networks," Proc. Second Symp. Networked Systems Design and Implementation, Apr. 2005.
23. 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.
24. M. Mathis, J. Mahdavi, S. Floyd, and A. Romanow, "RFC 2018—TCP Selective Acknowledgement Options," technical report, PSC, LBNL, Sun Microsystems, Oct. 1996.
25. D.B. Johnson, "ECC, Future Resiliency and High Security Systems," white paper, Certicom, www.certicom.com, Mar. 1999.
26. Y. Hu, D.B. Johnson, and A. Perrig, "SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks," Ad Hoc Networks, vol. 1, no. 1, pp. 175-192, 2003.
27. L. Lamport, "Password Authentication with Insecure Communication," Comm. ACM, vol. 24, no. 11, pp. 770-772, Nov. 1981.
28. C.E. Perkins and P. Bhagwat, "Highly Dynamic Destination- Sequenced Distance-Vector Routing (DSDV) for Mobile Computers," Proc. ACM Special Interest Group on Data Comm. (SIGCOMM '94), pp. 234-244, Aug. 1994.
29. R.L. Rivest, "RFC 1321—The MD5 Message-Digest Algorithm," technical report, MIT Laboratory for Computer Science and RSa Data Security, Inc., Apr. 1992.
30. D. Eastlake and P. Jones, "RFC 3174—US Secure Hash Algorithm 1 (SHA1)," technical report, Motorola and Cisco Systems, Sept.2001.
31. "The Network Simulator (ns-2)," http://www.isi.edu/nsnam/ ns/, 2005.

32. J.Y. Le Boudec and M. Vojnovi_c, “Perfect Simulation and Stationarity of a Class of Mobility Models,” Proc. INFOCOM, Mar. 2005.
33. R. Akbani, T. Korkmaz, and G. V. S. Raju, “Mobile Ad hoc Network Security,” in Lecture Notes in Electrical Engineering, vol. 127.New York: Springer-Verlag, 2012, pp. 659–666.
34. R. H. Akbani, S. Patel, and D. C. Jinwala, “DoS attacks in mobile ad hoc networks: A survey,” in Proc. 2nd Int. Meeting ACCT, Rohtak, Haryana, India, 2012, pp. 535–541.
35. T. Anantvalee and J. Wu, “A Survey on Intrusion Detection in Mobile Ad Hoc Networks,” in Wireless/Mobile Security. New York: Springer-Verlag, 2008.
36. L. Buttyan and J. P. Hubaux, Security and Cooperation in Wireless Networks. Cambridge, U.K.: Cambridge Univ. Press, Aug. 2007.
37. D. Dondi, A. Bertacchini, D. Brunelli, L. Larcher, and L. Benini, “Modeling and optimization of a solar energy harvester system for self-powered wireless sensor networks,” IEEE Trans. Ind. Electron., vol. 55, no. 7, pp. 2759–2766, Jul. 2008.
38. V. C. Gungor and G. P. Hancke, “Industrial wireless sensor networks: Challenges, design principles, and technical approach,” IEEE Trans. Ind. Electron., vol. 56, no. 10, pp. 4258–4265, Oct. 2009.