Journal of Research Proceedings

JRP

Under the delegate of "Journal of Research Proceedings," we anchor a bimonthly electronic journal enclosing the diverse realms of the educational research field. JRP is providing a platform for the researchers, academicians, professionals, practitioners, and students to impart and share knowledge in the form of high quality empirical and theoretical research papers, case studies, literature reviews, and book reviews.

JRP Publications
www.i-jrp.com
journalrp.editor@gmail.com
9353189468

Intrusion Detection System Using AODV For Securing Blackhole Attack and Grayhole Attack in MANETS

Harshavardhan K [1], Pannaga P [2] , Vishakha H C [3] , Prof. Tejashwini N [4]
[1,2,3]ISE Department, Sri Krishna Institute of Technology, B'lore-560090, India
[4] Faculty ISE Department, Sri Krishna Institute of Technology, B'lore-560090, India

ABSTRACT

The MANET is a sort of wireless connection that can be deployed without the use of equipment. It is a system of peer, infrastructure-free, flexible, and decentralised mobile nodes which are connected to one another. The goal of this study is to examine and improve the safety of MANET routing protocols using Ad hoc On Demand Distance Vectors (AODV). This methodology for identifying blackhole as well as grayhole attacks is reflected in the development of modifying the sequence number given in control packets, particularly Route Reply Packets (RREP), in order to determine blackhole and grayhole nodes and thus minimise loss of information by throwing away the route with so problems with nodes.

KEYWORDS: AODV, Black hole, receive reply, sequence number, routing table.

1. INTRODUCTION

Forwarding in ad hoc networks has a variety of obstacles such as high mobility and node density, which lead to significant loss in performance. Threats and intrusion prevention systems in MANETs are covered in this survey [1-5]. All nodes keeping their forwarding table updated with data broadcast from other sites. As a result, routing database overflow attacks may occur, causing the resource processes to be disrupted. Due to the extreme nature of a transit data concerned, responsive protocols such as AODV [6-11], are more resistant to replay assaults. We offer a technique to fight the AODV routing protocol's doubtfull threat [12].

By removing the requirement for centralised management MANETs allow a set of wirelessly capable nodes to communicate freely within their routing protocol and practically anyplace [13-14].

The Ad hoc On-Demand Distance Vector (AODV) networking system is a routing protocols technique extensively utilised in MANET [15-22]. The AODV transportation protocol is extremely susceptible to channeling assaults, particularly black hole attacks. Attacker node inject bogus networking data into the black hole, causing the original node to choose the route with both the suspect network as the optimal option. Malicious nodes receives packets of data and kills them completely, resulting in a Denial of Service (DoS) attacks [23-28].

With a newly developed data packet that matches the RREP packet destination address obtained from the blackhole station. If the answering node is a blackhole nodes, this will re-send an RREP message with an even greater data packet [29-34], indicating that it wants the packet from the origin to be forwarded through everything (and finally dropped) [35].

Getting RREP packet with such a larger series than first attempt confirms the nature of a problematic node, and routing through these nodes are dropped. As a result, the likelihood of packet loss lowers, resulting in improved system performance [36].

2.LITERATURE SURVEY

In MANET, there are 3 kinds of communication algorithms: I preemptive or table-driven, (ii) reactive or on-demand, and (iii) hybrid, which combines proactive and reactive procedures. Knowledge flow is encrypted and

recorded actively in a route cache that is preserved by every nodes. DSDV, WRP, FSR, and other proactive routing systems are examples. Responsive routing differs from traditional routing since it does not use a routing table. Only once and the need for that is the route created first before communication begins. The DSR and AODV are both well-known. ZRP is an example of a reactive and proactive procedure that is employed (Zone routing protocol). These protocols, on the other hand, are unsecure and vulnerable to a variety of assaults [37-38].

Various cryptography algorithms are utilised for MANET safety, each with advantages and disadvantages; nevertheless, one technique called Secret Sharing Schemes (SSS)/Key exchange protocol is effective for MANET safety. It is a type of encryption that allows a private value to be negotiated from private shares/public communications. In ad-hoc situations, this agreement key

could be utilised for symmetrical encryption and decryption. Public - key cryptography can also serve as an environment for encapsulating and negotiating symmetrical secret keys among endpoints [39-40].

The researchers of introduced a new method for detecting and eliminating risky attacks without the use of any extra packets or packet header. When an original node gets RREP packets, it creates a new RREQ, assigns the best identifier to the new RREQ packet, and unicasts it over the same route as the preceding RREP packet.

When a malignant node receives an RREQ packet, it creates an RREP packet with such a greater data packet than the one it received. The rogue sender forwards the sender node a bogus RREP packet. The sender marks the RREP generation as harmful because the attacker user sends a series higher number than just its prior identifier. Without the use of any additional packets, this method may detect malicious nodes.

The authors proposed a method dependent on promiscuity mode in INs. Each nodes observes its neighbours and generates a threshold to identify phishing routers using this method. The limit is determined by the ratio of accepted to sent packets. This method can detect a single rogue node, that being said it can identify collaborative faulty activities that send packets of data to each other to bypass the security method.

3.METHODOLOGY

This protocol is composed of two mechanism

(1) Route Discovery and

(2) Route Maintenance.

In the Route Discovery phase, AODV employs Route Re Request (RREQ) and Route Reply (RREP) command communications, and in the Route Maintenance stage, it uses Route Error (RERR) data transmission. This control message's header data could be seen in full. The nodes involved in the connection might be characterised as sensor node, intermediary nodes, or destination nodes in generally. The behaviour of a nodes differs depending on the role. Whenever a sender needs to chat to a destination network, it first looks in the existent routing process to see if there is a new route to that target.

If a clean sufficient route is accessible it utilizes the very same. Instead, the node starts the Route Discovery process by sending an RREQ control message to all of its neighbours. The intermediary node will then transmit (again broadcast) this RREQ information to their neighbours. This process continues till a new route to the target is found at the destination node or an intermediary node

Working of AODV

FOR THE TARGET VISIBLE TO THE SOURCE NODE, THE RREQ INCLUDES THE NETWORK NODE IP ADDRESS, PRESENT SEQUENCE NUMBER, BROADCAST ID, AND MOST RECENT SEQUENCE NUMBER. THE TARGET NODE TERMINATES A ROUTE REPLY (RREP) PACKETS ALL ALONG BACKWARD DIRECTION CONSTRUCTED AT INTERMEDIARY NODES DURING ROUTE IDENTIFICATION PROCEDURE WHEN IT RECEIVES RREQ. A ROUTE ERROR (RERR) PACKET IS TRANSMITTED TO THE ORIGIN AND TARGET NODES IN THE EVENT OF A ROUTE FAILURES. A BASE STATION CAN ALWAYS LOCATE NEW VALID PATHS BY EMPLOYING SEQUENCE NUMBERS. FOR DYNAMIC ROUTING, AODV OFFERS THREE TYPES OF CONTROL MESSAGES.

Security Flaws in AODV

Because of the paper's potential applications, AODV is subject to routing attacks by malicious nodes. Although a conclusions may summarise the paper's primary ideas, it should not be a repeat of the abstract. A epilogue could expound on the significance of the work or suggest applications and extensions that are normally built to have capabilities like identification, authenticity, secrecy, and availability. AODV can easily be manipulated by a malicious node to disrupt its routing.

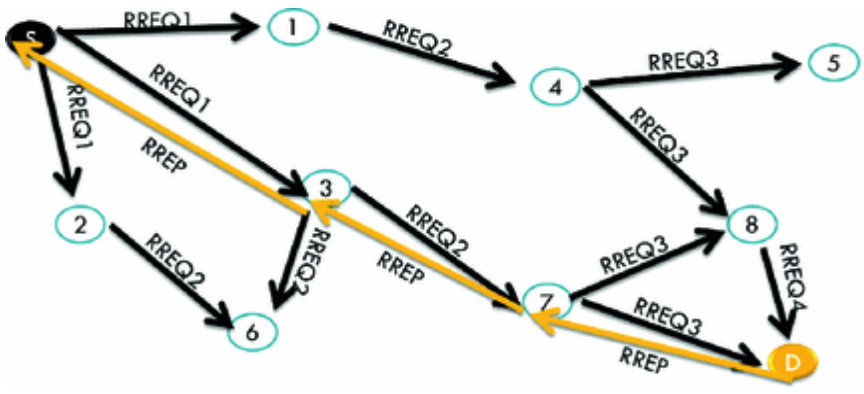

Figure 1: AODV Routing Protocol

4. IMPLEMENTATION

In this study, a novel solution to the issue of blackholes is proposed. A blackhole node is expected to occasionally to seem as the best next member nodes for the source network to reach the correct node. It accomplishes this by responding with an RREP packet with false data about having the lowest number of hops and the greatest sequence number, accordingly, whereby number of hops specifies the number of nodes between two points. The assaulting node raises the RREQ sequence value in the packets by a random number such as 100. The maximum Arbt value is thought to indicate a sudden or unusual increase in the sequence numbers indicating paths between mobile nodes. The proposed method tries to take use of this feature of a blackhole node, and then includes a methodology where a supplier node twice the amount result. the legitimacy of the intermediary nodes which responds via an RREP packet with a disturbingly large destination node. Whenever an origin node gets an RREP packet with a destination sequencing value is more than the expected Arbt from the origin sequence value. It resends the RREQ packet, however this moment with both the target sequence updated to the RREP packet's sequence number. Since the similar node sends another RREP packet with a surprisingly high destination sequence value the route is dropped.

Pseudo Code of Proposed Algorithm

Notations

SN: Source Node

IN: Intermediate Node RRq: Re-Broadcast RREQ

SSN: Source Sequence Number DSN: Destination Sequence Number Mal: Malicious Node

1. SN Broadcast RREQ

2. Wait for RREP

3. On Receiving RREP

*4. IF (RREP Sequence Number –SSN> Arbt*max *) {*

5. RRq by changing SSN to RREP sequence number

6. Wait for RREP

*7. IF (RREP Sequence Number – SSN > Arbt*max *) {*

8. Mal Detected

9. Discard the Route

10. }

11. }

12. ELSE {

13. Send the Data Using the Route

14. }

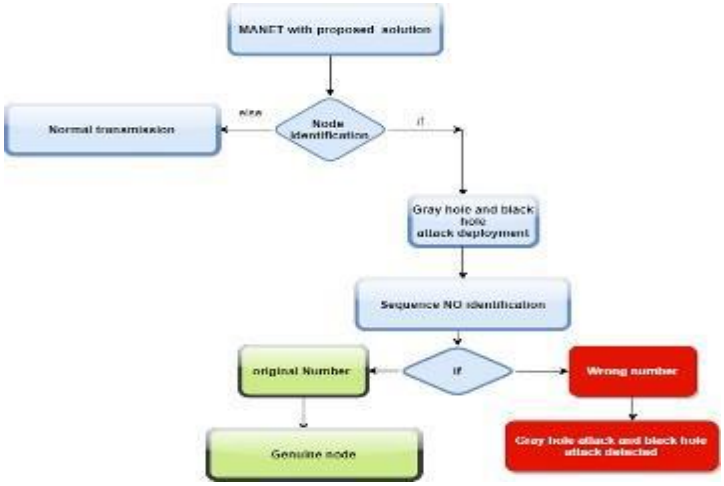

Figure 2: Block Diagram for malicious attack

Gray hole attack caused by RREP

The AODV routing protocol is a popular reactive routing protocol in wireless networks, but AODV routing protocol designed for better performance of the network not for security.

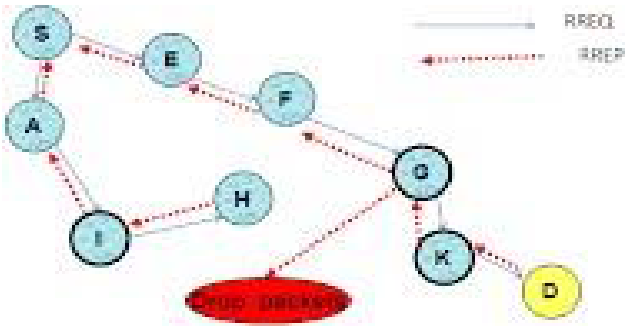

Figure 3: Gray hole attack

Black hole attack caused by RREP

The below figure 3 represents black hole attack caused by RREP

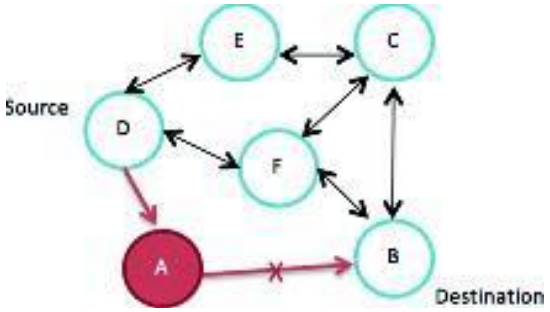

Figure 3: Black hole attack

CONCLUSION

The examination of a security problem known as a blackhole and grayhole in MANETs was described in this publication, along with its influence on the network. In addition, current solutions to the problem are examined, analysed, and a novel technique is offered as a result. In comparing to historical techniques, the suggested algorithm is quite basic and can perform well. The developed algorithm's effectiveness is also examined.

REFERENCES

[1] D. B. Johnson and D. A. Maltz, "Dynamic Source Routing in Ad Hoc," in Mobile Computing, vol. 5, C. P. Perkins, Ed., Kluwer Academic Publishers, 1996, pp. 153-181.

[2] Chakraborty, C., Roy, S., Sharma, S., Tran, T., Adhimoorthy, P., Rajagopalan, K. and Jebaranjitham, N., 2021. Impact of Biomedical Waste Management System on Infection Control in the Midst of COVID-19 Pandemic. The Impact of the COVID-19 Pandemic on Green Societiesenvironmental Sustainability, pp.235-262.

[3] Rachana, C.R., Banu, R., Ahammed, G.A. and Parameshachari, B.D., 2017, August. Cloud Computing–A Unified Approach for Surveillance Issues. In IOP Conference Series: Materials Science and Engineering (Vol. 225, No. 1, p. 012073). IOP Publishing.

[4] Chakraborty, C., Roy, S., Sharma, S., Tran, T., Dwivedi, P. and Singha, M., 2021. IoT Based Wearable Healthcare System: Post COVID-19. The Impact of the COVID-19 Pandemic on Green Societiesenvironmental Sustainability, pp.305-321.

[5] C. E. Perkins and E. M. Royer, "Ad-hoc on- demand distance vector routing," in Proceedings WMCSA'99. Second IEEE Workshop on Mobile Computing Systems and Applications, New Orleans, 1999.

[6] Sreevathsa, C.V., Daina, K.K., Hemalatha, K.L. and Manjula, K., 2016, July. Increasing the performance of the firewall by providing customized policies. In 2016 2nd International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT) (pp. 561-564). IEEE.

[7] Arun, M., Baraneetharan, E., Kanchana, A. and Prabu, S., 2020. Detection and monitoring of the asymptotic COVID-19 patients using IoT devices and sensors. International Journal of Pervasive Computing and Communications.

[8] Seyhan, K., Nguyen, T.N., Akleylek, S., Cengiz, K. and Islam, S.H., 2021. Bi-GISIS KE: Modified key exchange protocol with reusable keys for IoT security. Journal of Information Security and Applications, 58, p.102788.

[9] H. Fu and H. Weerasinghe, "Preventing cooperative black hole attacks in mobile ad hoc networks: Simulation implementation and evaluation," Future Generation Communication and Netwroking, vol. 2, pp. 362-367, 2007.

[10] Boregowda, S.B., Babu Prasad, N.V., Puttamadappa, C. and Mruthyunjaya, H.S., 2015. Energy Balanced Fixed Clustering protocol for Wireless Sensor Networks. International Journal of Computer Science and Network Security, 11(8), pp.166-172.

[11] L. Zhen, Y. Zhang, K. Yu, N. Kumar, A. Barnawi and Y. Xie, "Early Collision Detection for Massive Random Access in Satellite-Based Internet of Things," **IEEE Transactions on Vehicular Technology**, vol. 70, no. 5, pp. 5184-5189, May 2021, doi: 10.1109/TVT.2021.3076015.

[12] L. Tan, K. Yu, A. K. Bashir, X. Cheng, F. Ming, L. Zhao, X. Zhou, "Towards Real-time and Efficient Cardiovascular Monitoring for COVID-19 Patients by 5G-Enabled Wearable Medical Devices: A Deep Learning Approach", **Neural Computing and Applications**, 2021, https://doi.org/10.1007/s00521-021-06219-9.

[13] K. Yu, M. Arifuzzaman, Z. Wen, D. Zhang and T. Sato, "A Key Management Scheme for Secure Communications of Information Centric Advanced Metering Infrastructure in Smart Grid," **IEEE Transactions on Instrumentation and Measurement**, vol. 64, no. 8, pp. 2072-2085, August 2015.

[14] S. Chen, L. Zhang, Y. Tang, C. Shen, R. Kumar, **K. Yu**, U. Tariq, and A. K. Bashir, "Indoor Temperature Monitoring Using Wireless Sensor Networks: A SMAC Application in Smart Cities", **Sustainable Cities and Society**, vol. 61, p. 102333, July 2020.

[15] W. Zeng, Z. Guo, Y. Shen, A. K. Bashir, **K. Yu**, Y. D. Al-Otaibi, and X. Gao, "Data-Driven Management for Fuzzy Sewage Treatment Processes Using Hybrid Neural Computing", **Neural Computing and Applications**, https://doi.org/10.1007/s00521-020-05655-3.

[16] K. Yu, L. Tan, X. Shang, J. Huang, G. Srivastava and P. Chatterjee, "Efficient and Privacy-Preserving Medical Research Support Platform Against COVID-19: A Blockchain-Based Approach", **IEEE Consumer Electronics Magazine**, doi: 10.1109/MCE.2020.3035520.

[17] F. Ding, G. Zhu, M. Alazab, X. Li, and **K. Yu**, "Deep-Learning-Empowered Digital Forensics for Edge Consumer Electronics in 5G HetNets", **IEEE Consumer Electronics Magazine**, doi: 10.1109/MCE.2020.3047606.

[18] Bhuvaneswary, N., S. Prabu, S. Karthikeyan, R. Kathirvel, and T. Saraswathi. "Low Power Reversible Parallel and Serial Binary Adder/Subtractor." *Further Advances in Internet of Things in Biomedical and Cyber Physical Systems* (2021): 151.

[19] Nguyen, Ngoc-Tu, Bing-Hong Liu, Shao-I. Chu, and Hao-Zhe Weng. "Challenges, designs, and performances of a distributed algorithm for minimum-latency of data-aggregation in multi-channel WSNs." *IEEE Transactions on Network and Service Management* 16, no. 1 (2018): 192-205.

[20] Subramani, Prabu, Ganesh Babu Rajendran, Jewel Sengupta, Rocío Pérez de Prado, and Parameshachari Bidare Divakarachari. "A block bi-diagonalization-based pre-coding for indoor multiple-input-multiple-output-visible light communication system." *Energies* 13, no. 13 (2020): 3466.

[21] Bhuvaneswary, N., S. Prabu, K. Tamilselvan, and K. G. Parthiban. "Efficient Implementation of Multiply Accumulate Operation Unit Using an Interlaced Partition Multiplier." *Journal of Computational and Theoretical Nanoscience* 18, no. 4 (2021): 1321-1326.

[22] Z. Guo, Y. Shen, A. K. Bashir, M. Imran, N. Kumar, D. Zhang and **K. Yu**, "Robust Spammer Detection Using Collaborative Neural Network in Internet of Thing Applications", **IEEE Internet of Things Journal**, vol. 8, no. 12, pp. 9549-9558, 15 June15, 2021, doi: 10.1109/JIOT.2020.3003802.

[23] L. Tan, K. Yu, F. Ming, X. Cheng, G. Srivastava, "Secure and Resilient Artificial Intelligence of Things: a HoneyNet Approach for Threat Detection and Situational Awareness", **IEEE Consumer Electronics Magazine**, 2021, doi: 10.1109/MCE.2021.3081874.

[24] Hemalatha, K. L., S. M. Ashitha, and S. R. Meghana. "Design and implementation of modified FCM in the detection of brain tumor." *Int. J. Adv. Sci. Res. Eng* 3, no. 4 (2017): 2850-2858.

[25] Hemalatha, K. L., SUNILKUMAR MANVI, and HN SURESH. "ADAPTIVE WEIGHTED-COVARIANCE REGULARIZED KERNEL FUZZY C MEANS ALGORITHM FOR MEDICAL IMAGE SEGMENTATION." *Journal of Theoretical & Applied Information Technology* 95, no. 14 (2017).

[26] Nguyen, Ngoc-Tu, Ming C. Leu, and Xiaoqing Frank Liu. "RTEthernet: Real-time communication for manufacturing cyberphysical systems." *Transactions on Emerging Telecommunications Technologies* 29, no. 7 (2018): e3433.

[27] Rajendrakumar, Shiny, V. K. Parvati, B. D. Parameshachari, KM Sunjiv Soyjaudah, and Reshma Banu. "An intelligent report generator for efficient farming." In *2017 International Conference on Electrical, Electronics, Communication, Computer, and Optimization Techniques (ICEECCOT)*, pp. 1-5. IEEE, 2017.

[28] Pham, Dung V., Giang L. Nguyen, Tu N. Nguyen, Canh V. Pham, and Anh V. Nguyen. "Multi-topic misinformation blocking with budget constraint on online social networks." *IEEE Access* 8 (2020): 78879-78889.

[29] Manjanaik, N., B. D. Parameshachari, S. N. Hanumanthappa, and Reshma Banu. "Intra Frame Coding In Advanced Video Coding Standard (H. 264) to Obtain Consistent PSNR and Reduce Bit Rate for Diagonal Down Left Mode Using Gaussian Pulse." In *IOP Conference Series: Materials Science and Engineering*, vol. 225, no. 1, p. 012209. IOP Publishing, 2017.

[30] Do, Dinh-Thuan, Tu Anh Le, Tu N. Nguyen, Xingwang Li, and Khaled M. Rabie. "Joint impacts of imperfect CSI and imperfect SIC in cognitive radio-assisted NOMA-V2X communications." *IEEE Access* 8 (2020): 128629-128645.

[31] Parameshachari, B. D., H. T. Panduranga, and Silvia liberata Ullo. "Analysis and computation of encryption technique to enhance security of medical images." In *IOP Conference Series: Materials Science and Engineering*, vol. 925, no. 1, p. 012028. IOP Publishing, 2020.

[32] Nguyen, Tu N., Bing-Hong Liu, Nam P. Nguyen, and Jung-Te Chou. "Cyber security of smart grid: attacks and defenses." In *ICC 2020-2020 IEEE International Conference on Communications (ICC)*, pp. 1-6. IEEE, 2020.

[33] Rajendran, Ganesh B., Uma M. Kumarasamy, Chiara Zarro, Parameshachari B. Divakarachari, and Silvia L. Ullo. "Land-use and land-cover classification using a human group-based particle swarm optimization algorithm with an LSTM Classifier on hybrid pre-processing remote-sensing images." *Remote Sensing* 12, no. 24 (2020): 4135.

[34] Nguyen, Tu N., Bing-Hong Liu, and Shih-Yuan Wang. "On new approaches of maximum weighted target coverage and sensor connectivity: Hardness and approximation." *IEEE Transactions on Network Science and Engineering* 7, no. 3 (2019): 1736-1751.

[35] Rajendrakumar, Shiny, and V. K. Parvati. "Automation of irrigation system through embedded computing technology." In *Proceedings of the 3rd International Conference on Cryptography, Security and Privacy*, pp. 289-293. 2019.

[36] Subramani, Prabu, K. Srinivas, R. Sujatha, and B. D. Parameshachari. "Prediction of muscular paralysis disease based on hybrid feature extraction with machine learning technique for COVID-19 and post-COVID-19 patients." *Personal and Ubiquitous Computing* (2021): 1-14.

[37] Fathima, N., Ahammed, A., Banu, R., Parameshachari, B.D. and Naik, N.M., 2017, December. Optimized neighbor discovery in Internet of Things (IoT). In 2017 International Conference on Electrical, Electronics, Communication, Computer, and Optimization Techniques (ICEECCOT) (pp. 1-5). IEEE.

[38] Naeem, M.A., Nguyen, T.N., Ali, R., Cengiz, K., Meng, Y. and Khurshaid, T., 2021. Hybrid Cache Management in IoT-based Named Data Networking. IEEE Internet of Things Journal.

[39] M. Fihri, M. Otmani and A. Ezzati, "The Impact of Black-Hole Attack on AODV Protocol," International Journal of Advanced Computer Science and Applications, Special Issue on Advances in Vehicular Ad Hoc Networking and Applications , pp. 20-24, 2014.

[40] X. Chen and J. Wu, “Multicasting techniques in mobile ad-hoc networks”, The Handbook of Ad- hoc Wireless Networks, pp. 25–40, 2003.