Lecture Notes in Electrical Engineering

Volume 131

For further volumes:
http://www.springer.com/series/7818

Nabendu Chaki · Natarajan Meghanathan
Dhinaharan Nagamalai
Editors

Computer Networks & Communications (NetCom)

Proceedings of the Fourth International Conference on Networks & Communications

Springer

Editors
Nabendu Chaki
Department of Computer Science
and Engineering
University of Calcutta
Calcutta
India

Natarajan Meghanathan
Department of Computer Science
Jackson State University
Jackson
USA

Dhinaharan Nagamalai
Wireilla Net Solutions PTY Ltd
Albion, VIC
Australia

ISSN 1876-1100 ISSN 1876-1119 (electronic)
ISBN 978-1-4614-6153-1 ISBN 978-1-4614-6154-8 (eBook)
DOI 10.1007/978-1-4614-6154-8
Springer New York Heidelberg Dordrecht London

Library of Congress Control Number: 2012953117

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

Preface

The Fourth International Conference on Networks and Communications (NETCOM 2012) has been held in Chennai, India during December 22–24, 2012. The conference is proved to stimulate researchers from different parts of the world to exchange their ideas in the field of computer networks and data communications including various applications of these. The goal of this conference is to bring together researchers and practitioners from academia and industry to focus on understanding the domain of computer networking and communication technology toward establishing new collaborations in these areas. Authors invited to contribute by submitting original research articles that illustrate research results, projects, survey works, and industrial experiences describing significant advances in the relevant areas.

The conference organizing committee of the NETCOM 2012 took great initiative and interest in circulating the Call for Papers (CFP) for the conference. This effort resulted in a large number of submissions from the researchers of the leading International Universities and Institutes of 32 countries across the world. All the submissions underwent a tough and careful peer-review process with voluntary participation of the committee members and external expert reviewers. The papers had been reviewed based on the novelty of the contributions, technical content, organization, and clarity in presentation. The entire process of initial paper submission, review, and acceptance processes was done electronically. All these efforts undertaken by the Organizing and Technical Committees led to an exciting, rich, and a high-quality technical conference program. The NETCOM 2012 conference featured high-impact presentations for all attendees to enjoy, appreciate, and expand their expertize in the latest developments in Networks and Communications research.

The Technical Program Committee for the conference has selected only 84 papers for publication out of a total 469 number of submissions. The conference proceeding has been organized as a collection of papers presented in the order in which the papers appear in the final technical program for NETCOM 2012. We would like to take this opportunity to thank the General Chairs of NETCOM 2012. We are thankful to all the members of the Technical Program Committee and the

external reviewers for their excellent and tireless work. We would also thank Springer for the strong support and the authors who contributed to the success of the conference. Last, but not the least, on behalf of Steering Committee of NETCOM 2012, we sincerely wish that all attendees had been benefited scientifically from the conference. Indeed, we would consider ourselves worth of organizing such an event to offer a platform for all of you if some of tomorrow's works of excellence find its roots initiated from the podium of NETCOM 2012.

Nabendu Chaki
Natarajan Meghanathan
Dhinaharan Nagamalai

Organization Committee

General Chairs

Sanguthevar Rajasekaran	University of Connecticut, USA
Henrique Joao Lopes Domingos	University of Lisbon, Portugal

Steering Committee

Brajesh Kumar Kaushik	Indian Institute of Technology Roorkee, India
Natarajan Meghanathan	Jackson State University, USA
Nabendu Chaki	University of Calcutta, India
Rakhesh Singh Kshetrimayum	Indian Institute of Technology Guwahati, India
Dhinaharan Nagamalai	Wireilla Net Solutions PTY Ltd, Australia
Salah M. Saleh AL-MAJEED	University of Essex, United Kingdom

Program Committee Members

Michal Wozniak	Wroclaw University of Technology, Poland
Jacques DEMERJIAN	Communications and Systems, France
Jan Zizka	SoNet/DI, FBE, Mendel University in Brno, Czech Republic
Sarmistha Neogy	Jadavpur University, India
Yannick Le Moullec	Aalborg University, Denmark
Hwangjun Song	Pohang University of Science and Technology, South Korea
Krzysztof Walkowiak	Wroclaw University of Technology
Ioannis Karamitsos	University of Aegean, Greece
Ramayah	Universiti Sains Malaysia, Malaysia
Khoa N. Le	Griffith School of Engineering, Australia
T. G. Basavaraju	National Institute of Technology Karnataka (NITK), India

Solange Rito Lima	University of Minho, Portugal
Sherif S. Rashad	Morehead State University, USA
Dhinaharan Nagamalai	Wireilla Net Solutions PTY Ltd, Australia
David C. Wyld	Southeastern Louisiana University, USA
Selma Boumerdassi	Cnam/cedric, France
H. V. Ramakrishnan	Bharath University, India
Sattar B. Sadkhan	University of Babylon, Iraq
Eric Renault	Institut Telecom-Telecom SudParis, Evry, France
Alvin Lim	Auburn University, USA
Debasis Giri	Haldia Institute of Technology, India
S. Li	Swansea University, UK
Rushed Kanawati	LIPN-University Paris 13, France
Cristina Ribeiro	University of Waterloo, Canada
Alexander Ferworn	Ryerson University, Canada
Samiran Chattopadhyay	Jadavpur University, India
Rajarshi Roy	IIT, Kharagpur, India
S. A. V. Satyamurty	Indira Gandhi Centre for Atomic Research, India
Laiali Almazaydeh	University of Bridgeport, USA
Shrikant K. Bodhe	Bosh Technologies, India
Alireza Mahini	Islamic Azad University-Gorgan, Iran
N. K. Choudhari	Smt. Bhagwati Chaturvedi College of Engineering, India
Christos Politis	Kingston University, UK
Ayman Khalil	Institute of Electronics and Telecommunications of Rennes, France
Sridharan	CEG Campus-Anna University, India
Mohamed Hassan	American University of Sharjah, UAE
Zuqing Zhu	Cisco Systems, USA
Quan (Alex) Yuan	University of Wisconsin-Stevens Point, USA
Henrique J. A. Holanda	UERN-Universidade do Estado do Rio Grande do Norte, Brazil
Ajay K. Sharma	Dr. B R Ambedkar National Institute of Technology-India
Shrirang A. Kulkarni	National Institute of Engineering, India
Shin-ichi Kuribayashi	Seikei University, Japan
Abdel Salhi	University of Essex, United Kingdom
Antonio Liotta	Eindhoven University of Technology, The Netherlands
Emmanuel Jammeh	University of Plymouth, United Kingdom
Ghaida Al-Suhail	Basrah Univirsity, Iraq
Hao-En Chueh	Yuanpei University, Taiwan, R.O.C
John Woods	University of Essex, United Kingdom
J. K. Mandal	University of Kalyani, India
Ken Guild	University of Essex, United Kingdom
Martin Fleury	University of Essex, United Kingdom

Mohammad M. Banat	Jordan University of Science and Technology, Jordan
Nadia Qadri	University of Essex, United Kingdom
S. Hariharan	J.J.College of Engineering, India
Yasir Qadri	University of Essex, United Kingdom
Wichian Sittiprapaporn	Mahasarakham University, Thailand
Mahi Lohi	University of Westminster, UK
Houcine Hassan	Univeridad Politecnica de Valencia, Spain
Mohammed Ghanbari	University of Essex, United Kingdom
Abdulrahman Yarali	Murray State University, USA
Asmaa Shaker Ashoor	Babylon University, Iraq
Chin-Chih Chang	Chung Hua University, Taiwan
Doina Bein	The Pennsylvania State University, USA
Hossein Jadidoleslamy	University of Zabol, Iran
Kayhan Erciyes	Izmir University, Turkey
M. Mohamed Ashik	Salalah College of Technology, Oman
Mohamed Fahad AlAjmi	King Saud University, Saudi Arabia
Moses Ekpenyong	University of Edinburgh, Nigeria
Natarajan Meghanathan	Jackson State University, USA
Nazmus Saquib	University of Manitoba, Canada
Ruchi Tuli	Yanbu University College, Kingdom of Saudi Arabia
Selwyn Piramuthu	University of Florida, USA
Serguei A. Mokhov	Concordia University, Canada
Rituparna Chaki	West Bengal University of Technology, India
V. Sundarapandian	Vel Tech Dr. RR & Dr. SR Technical University, India
Pinaki Sarkar	Jadavpur University, India
S. Taruna	Banasthali University, India
S. Rajaram	Thiagarajar College of Engineering, India
Uday nuli	Textile and Engineering Institute Ichalkaranji, India
Shun HATTORI	Muroran Institute of Technology, Japan
Yoram Haddad	Jerusalem College of Technology/Ben Gurion University, Israel
Cathryn Peoples	University of Ulster, United Kingdom
Antonio Ruiz-Martinez	University of Murcia, Spain
Paulo R. L. Gondim	University of Brasilia, Brazil
Josip Lorincz	University of Split, Croatia
Jose-Fernan Martinez-Ortega	Universidad Politecnica de Madrid-UPM, Spain
Noor Zaman	King Faisal University, Saudi Arabia
Hangwei	Western Reserve University, USA
Nuno M. Garcia	Universidade Lusofona de Humanidades e Tecnologias, Portugal
Rachida Dssouli	Concordia University, Canada

Jaime Lloret	Polytechnic University of Valencia, Spain
Daqiang Zhang	Nanjing Normal University, China
Juan Jose Martinez Castillo	Ayacucho University, Venezuela
Malamati Louta	University of Western Macedonia, Greece
Malka N. Halgamuge	The University of Melbourne, Australia
Jose Neuman de Souza	Federal University of Ceara, Brazil
Iwan Adhicandra	University of Pisa, Italy
Bob Natale	MITRE, USA
Hamza Aldabbas	De Montfort University, UK
Behnam Dezfouli	University Technology Malaysia (UTM), Malaysia
Ehsan Heidari	Islamic Azad University Doroud Branch, Iran
Jadidoleslamy	University of Zabol, Iran
M. Nadeem Baig	King Saud University, K.S.A
Nisar Hundewale	University of Maryland University College, USA
Omar Almomani	Jadara University, Jordan
Paulo Martins Maciel	Federal University of Pernambuco, Brazil
Phan Cong Vinh	NTT University, Vietnam
Raed alsaqour	Universiti Kebangsaan Malaysia, Malaysia
Sajid Hussain	Fisk University, USA
Sherimon P. C.	Arab Open University, Sultanate of Oman
Somayeh Mohammadi	Islamic Azad University, Iran

Committee Members/Reviewers

A. V. N. Krishna	PJMS CET, India
Vijaya Raju M.	Epoka University (RINAS Campus), Europe
Abbas Aahmad	Hi-Tech College of Engineering and Technology, India
Amandeep Verma	Punjabi University, India
Amanpreet Kaur	ITM University, India
Amitava Mukherjee	BM GBS, India
Anand Kumar	Babasaheb Bhimrao Ambedkar (A Central) University, India
Anitha Vaddinuri	Sree Vidyanikethan Engineering College, India
Anjan K.	RVCE, India
Ankit Agarwal	PICT, India
Ankit Thakkar	Nirma University, India
Annappa	NITK, India
Arvind Kumar Sharma	Sine International Institute of Technology, India
Ashutosh Kumar Dubey	Trinity Institute of Technology and Research, India
B. K. Pattanayak	SOA Deemed to be University, India
Bhaskar Biswas	Banaras Hindu University, India

C. Mala	National Institute of Technology, India
D. Shravani	MIPGS, India
D. Srinivasa Rao	VNRVJIET, India
D. C. Dhubkarya	BIET JHANSI, India
Debabrata Singh	ITER, SOA University, India
Demian Antony D'Mello	St. Joseph Engineering College, India
Dhanalaxmi R.	Anna University Chennai, India
Divya T. V.	MG University India
Ferdinant T.	Jayaram College of Engineering and Technology, India
G. Sankara Malliga	VELS University, India
Gaikwad Dhananjay S.	HSBPVT's Parikrama College of Engineering, India
Gopalakrishnan Kaliaperumal	Anna University, India
Gosta Biswas	Indian School of Mines, India
Himanshu Sharma	GLNAIT Mathura, India
Indumathi	Anna University, India
Jayadev Gyani	Jayamukhi Institute of Technological Sciences, India
Jitendra Maan	Tata Consultancy Services, India
K. Vimala Devi	Kalasalingam University, India
Kahkashan Tabassum	Muffakham Jah College of Engineering and Technology, India
Kamlesh Dutta	National Institute of Technology, India
Kavuri.Roshan	J.B. Institute of Engineering and Technology, India
Khalid NASR	IRIT, India
Koteswara Rao G.	MSBI-HCL, India
Kousik Mukherjee	B.B.College, India
Latha Gannarapu	Kakatiya University, India
M. Upendra Kumar	Mahatma Gandhi Institute of Technology (MGIT), India
Mala	National Institute of Technology, India
Manjula Shenoy K.	MIT, India
Md. Mahmudul Hasan	Daffodil International University, Bangladesh
Minal moharir	R V College of Engineering, India
Mohd Dilshad Ansari	Invertis University, India
Mrinal Naskar	Jadavpur University Kolkata, India
Muttanna Kadal H. K.	Dr. AIT, India
N. Bhalaji	PERI Institute of Technology, India
Naishita Taraka	JNTU, India
Nandini Mukherjee	Jadavpur University, India
Neetesh	Indian Institute of Technology Indore, India
Nishant doshi	National Institute of Technology, India
Nityananda Sarma	Tezpur University, India

PESN. Krishna Prasad	Prasad V. Potluri Siddhartha Institute of Technology, India
P. Perumal	Sri Ramakrishna Engineering College, India
P. R. S. M. Lakshmi	Vignan University, India
Pankaj Sharma	ABES Engineering College Ghaziabad, India
Parveen kumar	Lovely Professional University, India
Poonam Garg	Institute of Management Technology, India
Pradeep	Sri Venkateshwara College of Engineering and Technology, India
Pranay Meshram	St. Vincent Palloti College of Engineering and Technology, India
Prasad Halgaonkar	MIT College of Engineering, India
Preetee K. Karmore	YCCE-Engineering College, India
R. Venkadeshan	Chettinad College of Engineering and Technology, India
R. Deepa	Amrita Vishwa Vidyapeetham, India
R. Selvarani	M S Ramaiah Institute of Technology, India
Racing Ruso	Anna University, India
Rahul Johari	Guru Gobind Singh Indraprastha University, India
Rajeshwari Hegde	BMS College of Engineering, India
RavendraSingh	MJP Rohilkhand University, India
Revathi	SRM University, India
Richard William	Jayalakshmi Institute of Technology, India
Ripal Patel	BVM Engineering College, India
S. Britto	Bharathidasan University, India
S. K. V. Jayakumar	Pondicherry University, India
Sandeep M. Chaware	D.J. Sanghvi College of Engineering, India
Sandhya Magesh	B.S.Abdur Rahman University, India
Santhi Thilagam	NITK Surathkal, India
Shahid Siddiqui	Integral University, India
Shaik Sahil Babu	Adavpur University, India
Sharmila Sankar	BSA Abdur Rahman University, India
Shatheesh sam	Nesamony Memorial Christian College, India
Shivaputra	Dr. Ambedkar Institute of Technology, India
Shriram K. Vasudevan	Amrita University, India
Siddesh G. M.	M.S. Ramaiah Institute of Technology, India
Soubhik Chakraborty	Birla Institute of Technology, India
Soumen Kanrar	Vehere Interactive Pvt Ltd, India
Sowmya	NITK, India
Srinivas	Jyothishmathi institute of Technology and Science, India
Subhrendu Guha Neogi	Sir Padampat Singhania University, India
Sunil Kumar Gupta	BCET GURDASPUR, India
T. Meyyappan	Alagappa University, India

T. P. Surekha	Vidya Vardhaka College of Engineering, India
Tapalina Bhattasali	West Bengal University of Technology, India
Tumpa Roy	GLA Groups of Institutions, India
Urmila Shrawankar	G H Raisoni College of Engineering, India
Utpal Biswas	University of Kalyani, India
V. Jayalakshmi	Sudharsan Engineering College, India
Vasu K.	IIT Kharagpur, India
Vijay H. Mankar	Government Polytechnic, India
Vikas J. Dongre.	Government Polytechnic, India
Vivekanand Mishra	S.V. National Institute of Technology, India
Vivekanandan Mahadevan	SRM University, India
Y. Srinivasa Rao	Andhra University College of Engineering, India
Y. Venkataramani	Saranathan College of Engineering, India
Zeenat Rehena	Jadavpur University,India
Zulfa Shaikh	Acropolis Institute of Technology and Research, India
Srinivasarao	Defence University College, Ethiopia
Zheng Chang	University of Jyvaskyla, Finland
Mohammad Zunnun Khan	Integral University, India
Gaurav Somani	LNMIIT, India
Mohammad	University of Botswana, Botswana
M. Sandhya	B.S. Abdur Rahman University, India
Elboukhari Mohamed	University Mohamed First, Morocco
Durgesh Samadhiya	Chung Hua University, Taiwan
Abbas Ahmad	Hi-Tech College of Engineering & Technology, India
Anu Bala	Chandigarh Engineering College, India
B. Jagadeesh	G.V.P. College of Engineering, India
Er. Saba Khalid	Integral University, India
Gagan Jindal	Chandigarh Engineering College, India
Hameem Shanavas	MVJ College of Engineering, India
Indrajit Banerjee	BESU, Shibpur, India
K. Kishan Rao	Vaagdevi Group of Technical Institutions, India
K. Suganthi	Madras Institute of Technology, India
Kaushik	IIT Kharagpur, India
Neeraj Kumar	Thapar University, Patiala (Punjab), India
P. Suresh Varma	Adikavi Nannaya University, India
Prabu D.	NetApp Inc., India
Prasun Chowdhury	Jadavpur University, India
R. R. Mudholkar	Shivaji University, India
Rajashree Biradar	Bellary Institute of Technology, India
RaviShankar Yadav	CAIR DRDO, India
Salil Kumar Sanyal	Jadavpur University, India
Samarendra Nath Sur	Sikkim Manipal Institute of Technology, India
Sanjay M. Koli	E & TC Department SKNCOE, India

Sarbani Roy	Jadavpur University, India
Seema Verma	Banasthali University, India
Shailaja kanawade	Sandip Institute of Technology and Research Centre, India
Sudesh	Sri Mata Vaishno Devi University, India
Vanathi B.	Anna University Chennai, India

Contents

Part I
The Fourth International Conference on Networks & Communications (NETCOM-2012): Adhoc and Sensor Networks

Perspectives of Sybil Attack in Routing Protocols of Mobile Ad Hoc Network

Manu Sood and Amol Vasudeva

Abstract It is cumbersome to achieve the security in a mobile ad hoc network due to its open nature, dynamically changing topology, lack of infrastructure and central management. A particular harmful attack that takes the advantage of these characteristics is the Sybil attack, in which a malicious node illegitimately claims multiple identities. Two routing mechanisms vulnerable to the Sybil attack in the mobile ad hoc networks are multi-path routing and geographic routing. In addition to these routing protocols, we show in this paper that the Sybil attack can also disrupt the head selection mechanism of various cluster-based routing protocols such as lowest id, highest node degree and mobility based clustering. To achieve this, we illustrate to have introduced a category of Sybil attack in which the malicious node varies its transmission power to create a number of virtual illegitimate nodes called Sybil Nodes, for the purpose of communication with legitimate nodes of the MANETs.

Keywords Mobile ad hoc network · Sybil attack · Malicious node · Sybil node · Network security · Routing protocol

1 Introduction

Security is an important concern in the Mobile Ad hoc Networks (MANETs). However, the characteristics of MANETs pose both challenges and opportunities in achieving the security goals, such as confidentiality, authentication, integrity,

M. Sood
Department of Computer Science, Himachal Pradesh University,
Shimla, Himachal Pradesh, India

A. Vasudeva (✉)
Department of Computer Science and Engineering and Information Technology,
Jaypee University of Information Technology, Waknaghat,
Solan, Himachal Pradesh, India
e-mail: amol_dev@rediffmail.com

N. Chaki et al. (eds.), *Computer Networks & Communications (NetCom)*,
Lecture Notes in Electrical Engineering 131, DOI: 10.1007/978-1-4614-6154-8_1,

availability, access control and non-repudiation [1]. There are a wide variety of attacks that target the weakness of MANET routing protocols. Most sophisticated and subtle routing attacks have been identified in some recently published papers such as Blackhole [2], Rushing [3], wormhole [4] and Sybil attack [5] etc. A Sybil attack is an attack [5], in which a malicious node illegally claims multiple identities by impersonating other nodes or by claiming fictitious identities. Sybil attacks are also capable of disrupting the routing mechanisms in mobile ad hoc networks. Karlof and Wagner have shown in [6] that multi-path routing and geographical routing schemes are affected by this attack. In case of multi-path routing a set of supposedly disjoint paths can all be passing through the same malicious node, which is using several Sybil identities. Also in location based routing a malicious node can present multiple Sybil nodes with different positions to its neighbors. Therefore, a legitimate node may choose any of the Sybil nodes while forwarding the packet on the basis of nearest location to the destination node; but in reality it will be passing the packets through the malicious node.

In addition to these routing protocols, we have shown in this paper that the Sybil attack can also disrupt the head selection mechanism of various cluster-based routing protocols such as lowest ID [7], highest node degree [8] and mobility based clustering [9]. To the best of our knowledge, this is for the first time that the impact of Sybil attack has been shown in these cluster based routing algorithms. The rest of this paper is organized as follows. Section 2 describes the Sybil attack in details. Section 3 describes the following routing protocols: Split Multi-path Routing (SMR) [10], Greedy Perimeter Stateless Routing (GPSR) [11] and various cluster based routing protocols along with the effect of Sybil attack on these protocols, respectively. Finally, the Sect. 4 concludes the paper.

2 Sybil Attack

Sybil attack was first introduced by J. R. Douceur. According to Douceur, the Sybil attack is an attack by which a single entity can control a substantial fraction of the system by presenting multiple identities [5]. The Sybil attack can occur in a distributed system that operates without a central authority to verity the identities of each communicating entity [12].

In a Mobile Ad hoc Network, the only way for an entity to detect the presence of other entities is by sending and receiving the messages over a shared broadcast communication channel. By taking the advantage of this feature, a malicious node can send messages with multiple fake identities. The node spoofing the identities of the nodes is called malicious node/Sybil attacker, and the nodes whose identities are spoofed are called Sybil nodes. Figure 1 represents a malicious node S along with its four Sybil nodes (S_1, S_2, S_3 and S_4). If this malicious node communicates with any legitimate node by presenting all its identities, the legitimate node will have illusion that it has communicated with five different nodes. But in actual, there exists only one physical node with multiple different IDs. If a single malicious node is able to

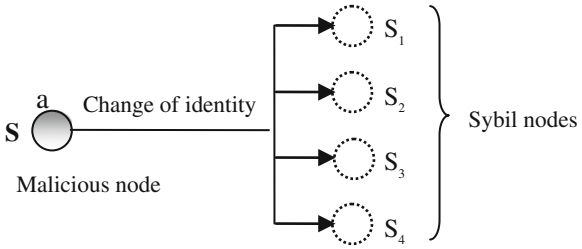

Fig. 1 A Sybil attacker with multiple IDs

convince its neighbors by presenting multiple identities, it will have control over the substantial portion of the network and can adversely affect the functioning of the network. According to Newsome [12], the mechanisms that are affected by the Sybil attack are: Data Aggregation, Fair Resource Allocation, Voting and Misbehavior Detection etc. Karlof and Wagner have shown in [6] that Sybil attack can also disrupt the functioning of certain routing protocols in MANETs such as multi-path routing protocols [10, 13, 14] and geographic based routing protocols [11, 15, 16].

The launching of the Sybil attack can be represented using three dimensions: Communication, Participation and Identity [12]. Newsome et al. state that there are two ways of communication: Direct and Indirect [12]. In a direct communication, as the name implies, the malicious node allows its Sybil nodes to communicate directly with the legitimate nodes. In case of indirect communication, the malicious node does not allow its Sybil nodes to communicate directly with the legitimate nodes. However, the authors are of the opinion that the title 'Establishment of the Connection' would have been more appropriate instead of the title 'Communication'. Participation is concerned about the participation of Sybil nodes in the communication with legitimate nodes in the network. These nodes can participate simultaneously or non-simultaneously. There are two methods by which a Sybil node can get the identity: In the first method a Sybil node can steal the identity of a legitimate node by impersonating it. The second method involves the fabrication of a fresh fake identity.

3 Sybil Attack in MANET Routing Protocols

In this section, we have illustrated the impact of Sybil attack on Split Multi-path Routing (SMR) and Greedy Perimeter Stateless Routing (GPSR). In addition to these routing protocols, we have shown that the Sybil attack can also disrupt the different forms of Cluster Based Routing Protocols such as Lowest ID Clustering, Highest Node Degree Clustering and Mobility based Clustering.

3.1 Sybil Attack in Split Multi-Path Routing (SMR)

Split Multi-path Routing (SMR) [10], one of the multi-path routing protocols based on Dynamic Source Routing (DSR) [17], establishes and utilizes multiple maximally disjoint paths. Unlike DSR, the intermediate nodes in SMR do not respond to route requests, in order to obtain maximal node disjoint paths. Intermediate nodes forward the first RREQ they receive and instead of dropping all the duplicate RREQ packets, rebroadcast those duplicate packets that are being received through a different incoming link and whose hop count is not greater than the previously received RREQs. When the destination node receives the first RREQ, it responds with RREP to the source node and then waits for certain duration of time, to receive additional requests. The destination node then selects the route that is maximally disjoint to the route that is already replied. Consider Fig. 2a, where the source node S floods the RREQ packets to find an optimal route to the destination node D. The intermediate nodes forward the duplicate RREQ packets that traversed through a different incoming link than the link from which the first RREQ is received, and whose hop count is not greater than that of the first received RREQ. Now assume that a Sybil attacker node M has established itself in the network with two fake IDs i.e. X and Y. Thus, in this case the packets are being forwarded through a single physical node i.e. M. When

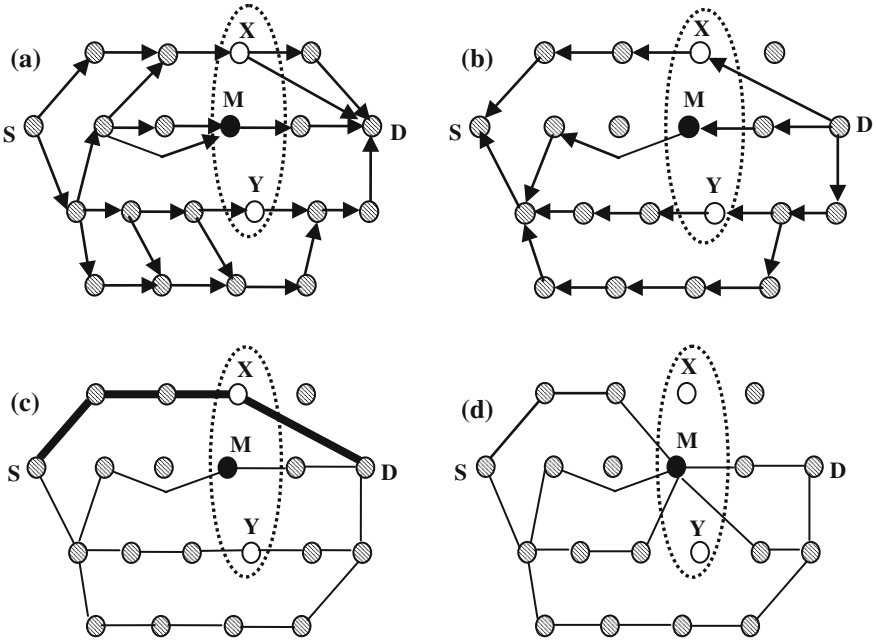

Fig. 2 **a** Flooding of RREQ packet from S to D. **b** RREP packets from D to S. **c** Selections of multiple disjoint paths. **d** Routes passing through the same node M. **S**-Source Node, **D**-Destination Node, **M**-Malicious Node, **X**, **Y**-Sybil Nodes

the RREQ packets have started to arrive at the destination node, it starts to send the RREP packets back towards the source node (Fig. 2b).
The path followed by each RREP packets is same as that of their corresponding RREQ packets. After receiving all the RREP packets the source node S makes the entry in its routing table. It then chooses the route with minimum hop count of 4 as shown in Fig. 2c by a thick line. But in reality, three routes are being passed through the same malicious node M and the Fig. 2d depicts that the routing mechanism has been disrupted, effectively.

3.2 Sybil Attack in GPSR Routing

The Greedy Perimeter Stateless Routing (GPSR) algorithm [11] works in two modes: greedy forwarding and perimeter forwarding. The algorithm starts forwarding with the greedy mode, by default. In greedy forwarding the source node looks for its neighbor that is closest to the destination and forwards the packet to that node. This process is repeated for the next node also and so on. Consider a MANET topology with 11 nodes as shown in the Fig. 3. Assume that the node C is a malicious node or Sybil attacker who somehow has succeeded to enter into the network. The actual position of this node is (7, 9). This node has presented two fake IDs i.e. the Sybil nodes D, E with their locations as (4, 11) and (11, 8), respectively. The node communicates with the other neighbors in its region by providing all the three locations (one actual and two fake). Thus, an adversary may claim to be present at more than one location for its neighbors by sending multiple HELLO messages, each time with different location information. Now suppose that the node A wants to send the packet to the destination I and to find the route it follows the greedy forwarding. A's radio range is denoted by the dotted circle about A and the arc with the radius equal to the distance between A and I is shown as arc about I. The node A forwards the packet to the Sybil node E, as it finds that the distance between E and I is less than between E and any of the A's other neighbors, according to the location information available in its Table 1. But in fact, node A has forwarded the packet to node C whose location is (7, 9) having a distance greater than the distance from node D (8, 2). Therefore, the routing scheme has been disrupted in the MANET with the entry of Sybil attacker.

3.3 Sybil Attack in Cluster-Based Routing Protocols

A Sybil attacker can also send the messages by varying its transmission power for all of its identities. The advantage of varying the transmission power for all the Sybil nodes is that the received signal strength at the receiving node with respect to these Sybil nodes will also be different. We have used the feature of variable transmission power to show that the Sybil attack can also disrupt various cluster based routing schemes such as lowest ID, highest node degree and mobility based clustering.

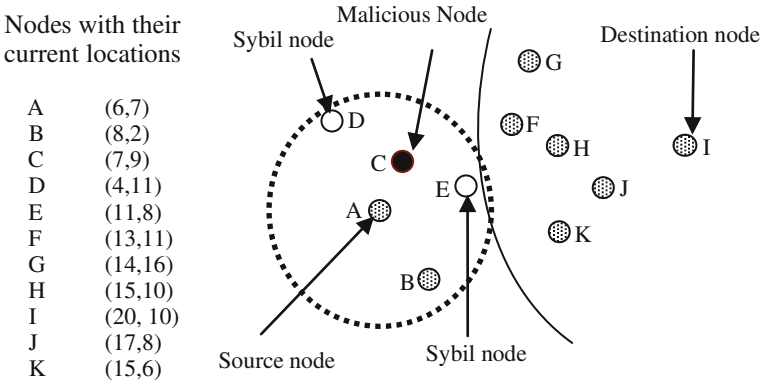

Fig. 3 A MANET topology with 11 nodes

Table 1 Location information of A's one hop neighbors

Neighbors of the source node A	Locations of A's neighbors	Distance of A's neighbors from the destination node I [10, 20]
B	(08, 02)	14.42
C	(07, 09)	13.04
D	(04, 11)	16.03
E	(11, 08)	09.22

Sybil Attack in Lowest ID Clustering Algorithm. In lowest ID algorithm [7], a node with the minimum ID is chosen as a clusterhead. Each node is provided with a unique ID and it periodically broadcasts the list of its neighbor's IDs, including itself. A node which only hears nodes with ID higher than itself is a clusterhead (CH).

Figure 4a shows a schematic of the result of using lowest ID clustering. There are 11 nodes with unique IDs, which form a connected graph. After the Lowest-ID clustering algorithm is executed, three clusters are formed, as depicted by the dotted circles. The black colored balls inside each cluster represent the clusterheads (1, 5 and 3 in Fig. 4). The striped balls (6 and 7) that are within the communication range of two or more different clusters represent the gateway nodes and the empty balls are the member nodes.

To become a cluster head, a malicious node can present the Sybil node with lowest ID in its neighborhood. For this, the malicious node will have to behave normally for the period until it has accessed the information about the whole network i.e. its one-hop, two-hop and n-hop neighbors and their respective IDs. After gaining the appropriate information, the malicious node can introduce its Sybil node with lowest ID, to fulfill its purpose by becoming the clusterhead. The attack becomes more devastating and difficult to be detected if the malicious node introduces its fake identities (Sybil nodes) by varying the transmission power. It takes the advantage of varying the transmission power in two ways: First, it cannot be detected on the basis

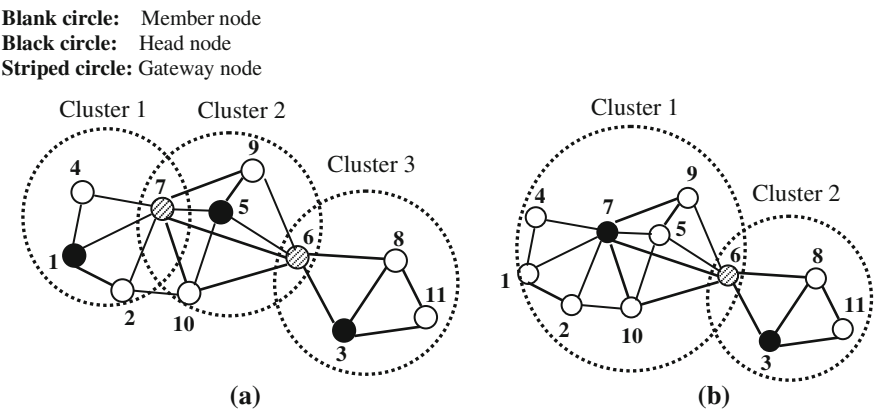

Fig. 4 Cluster formation process. **a** Lowest ID approach. **b** Highest node degree approach

of same signal strengths of its Sybil nodes [18]. Second, by decreasing the transmission power for different Sybil nodes, the message will not reach all the legitimate neighbors of the malicious node and hence cannot be detected on the basis of the fact that two different physical entities cannot have the same set of neighbors [19].

The Sybil attack can also disrupt the lowest ID based cluster routing by presenting multiple Sybil nodes with IDs higher than its neighboring legitimate nodes. Here the intention is to make the legitimate node with lowest ID, the clusterhead again and again to drain its battery. Once the battery is drained completely, the malicious node can impersonate its ID for one of its Sybil node to become a clusterhead.

Sybil Attack in Highest Node Degree Algorithm. In highest node degree algorithm [8], the degree of a node is computed on the basis of its neighbors. The node having maximum number of neighbors is elected as the clusterhead. If there is a tie between two or more nodes in terms of node degree, the node with lowest ID is chosen to be clusterhead. Figure 4b shows the result of using highest degree clustering for the same topology that was being used for the lowest ID algorithm.

The highest degree algorithm can also be disrupted by the Sybil attack. By presenting multiple Sybil nodes, a malicious node may claim to have more neighbors than the actual number. For example, in the Fig. 5, the node 5 is a malicious node with nodes 3, 4 and 6 as its one hop neighbors (hence node degree 3). The node 4 has the maximum node degree of 5 among its neighbors and should to be selected as a cluster head. But, the malicious node 5 also includes its three Sybil node, i.e. S_1, S_2 and S_3 so as to increase its node degree to 6 and hence becomes the clusterhead. Now the question is how to introduce these Sybil nodes to the legitimate neighboring nodes, i.e. with direct communication or indirect communication.

If indirect method of communication is followed, the malicious node will claim to have the specified number of Sybil identities as its neighbors and will not allow them to communicate directly with its legitimate neighboring nodes. But, due to mobile