International Journal of Engineering & Technology, 7 (3.8) (2018) 165-168

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Design and Implementation of Secure Routing Protocol in Mobile Ad Hoc Networks

Sachin Korde[1]*, Dr. Milind Sarode[2], Dr. V. M. Thakare[3]

[1]Research Scholar, SGBAU, Amravati
[2]Head of Department, Computer Engineering, Government Polytechnic, Yavatmal
[3]Head of Department, Department of Computer Science, SGBAU, Amravati
** E-mail: sachin.korde211@gmail.com*

Abstract

Security in Mobile Ad hoc NETworks (MANETs) is the most critical subject for the essential usefulness of the system. The accessibility of system administrations, classification and trustworthiness of the information might be accomplished by guaranteeing that security issues had been met. Versatile specially appointed Networks much of the time experience the ill effects of security assaults as a result of its highlights like open medium, changing its topology powerfully, loss of focal following and control, helpful calculations and no unmistakable guard component. Those components have changed the front line circumstance for the portable specially appointed Networks towards the security dangers. The portable specially appointed Networks work without an incorporated administration in which the hubs speak with each extraordinary based on common accept. This trademark makes portable specially appointed Networks additional inclined to be misused through an assailant in the system. Remote connections additionally make the portable impromptu Networks more noteworthy vulnerable to assaults, which make it easier for the assailant to move in the system and gain admittance to the continuous correspondence. Portable hubs show in the assortment of remote connection can catch or even take part in the system. Portable impromptu Networks ought to have a safe route for transmission and correspondence and that is a very difficult and fundamental issue as there's developing dangers of assault on the versatile Networks. Security is the call of the day. To relieve those issues, in this paper, we support another safe powerful hub validation plot for portable specially appointed systems condition to defeat security and protection issues in existing plans. We give the security three-part powerful hub verification convention for hub correspondence condition, which makes utilization of the elliptic bend cryptography (ECC). We moreover offer the security assessment of the proposed plot. This proposed plot is secure contrary to known assaults. The functional exhibit of the proposed plot is performed utilizing the broadly acknowledged NS2 reproduction instrument. The general execution of proposed conspire is enhanced as similar with the common plans.

Keywords: *Use about five key words or phrases in alphabetical order, Separated by Semicolon.*

1. Introduction

Mobil Ad hoc Networks are independent and decentralized remote frameworks. Portable impromptu Networks comprise of cell hubs which can be detached in moving inside and outside in the system. Hubs are the frameworks or gadgets i.e. cell phone, PC, private virtual help, MP3 player and private PCs that are working together inside the system and are cell. These hubs can go about as host/switch or each at the equivalent time. They can frame self-assertive topologies depending on their availability with each other in the system. Those hubs can possibly design themselves and because of their self-setup capacity, they might be sent critically without the need of any framework. Web Engineering Task Force (IETF) has Mobile Ad hoc Networks working gathering (WG) this is focused on creating IP steering conventions. Steering conventions are one of the testing and exciting exploration areas. Many directing conventions have been produced for cell specially appointed Networks, i.e. AODV, DSDV, DSR and numerous others[1].

Security in portable advert hoc organize is the most fundamental worry for the essential usefulness of the system. The accessibility of network contributions, classification and trustworthiness of the data might be finished by means of guaranteeing that security inconveniences have been met. cell advert hoc Networks regularly be tormented by security assaults in light of its capacities like open medium, changing its topology powerfully, loss of crucial checking and control, agreeable calculations and no unmistakable insurance instrument. These components have changed the front line situation for the portable specially appointed Networks against the security dangers.

The versatile impromptu Networks work without a concentrated administration in which the hubs talk with each extraordinary on the possibility of common trust. This capacity makes cell impromptu Networks additional at risk to be abused by an assailant in the network. Remote connections likewise make the cell specially appointed Networks more noteworthy powerless against assaults, which make it less troublesome for the aggressor to go inside the system and get right of passage to the progressing correspondence. Cell hubs display inside the scope of remote connection can catch or even take part inside the system. Versatile impromptu Networks need a comfortable way for transmission and correspondence and that is an entirely hard and imperative trouble as there might build dangers of attack on the cell Networks. Well-being is the call of the day[1].

With the goal to offer comfortable correspondence and transmission, the architects need to comprehend unique styles of assaults and their results at the portable specially appointed Networks. Wormhole assault, blackhole assault, Sybil assault, flooding assault, steering table flood strike, Denial of transporter (DoS), narrow minded hub getting out of hand, pantomime assault are the type of attacks that portable specially appointed Networks can experience the ill effects of. A portable specially appointed Networks is additional open to those styles of assaults because of the reality discussion depends on shared concur with between the hubs, there might be no basic point for network control, no approval office, overwhelmingly changing topology and limited resources.

2. Proposed Work

We proposed novel approach for secure dynamic node authentication and key agreement scheme which is a dynamic user authentication scheme for mobile ad hoc network node in which the base station node of the MANET and node dynamically authenticate one another. The safety analysis proved that the proposed system is secure. Moreover, we take a look at the configuration security substantiation concerning the proposed scheme towards blackhole attack, grayhole attack, man-in-the middle attacks.

In this section, we present a new three-factor dynamic node authentication protocol for node authentication environment, which uses the elliptic curve cryptography (ECC).

Suppose there is a node Ui wants to access the real-time data from a particular base station CNj. In this scenario, we require authentication between Ui and CNj . After mutual authentication between Ui and CNj, they establish a session key for the future secure communication. After this successful mutual authentication only, Ui can access the data in the network with the help of CNj.

In the proposed plot, we utilize the elliptic bend point duplication tasks. For better introduction of the paper, in the accompanying we show the fundamental properties of an elliptic bend, and its two essential tasks, for example, point expansion and point duplication. In elliptic bend cryptography (ECC), point increase (scalar duplication) is characterized as the rehashed point augmentations. For instance, if P? Ep(a, b), 5P is processed as 5P = P + P + P + P + P.

Given a scalar k?Zp and a point P? Ep (a, b), registering the scalar increase Q = k.P is moderately simple. Nonetheless, given P and Q in Ep(a, b), it is computationally infeasible to register the scalar k ?Zp, where Q = k.P . This issue is known as the elliptic bend discrete logarithm issue (ECDLP).

In this stage, a confided in specialist (TA) is in charge of enlisting each base station hub CNj and every hub preceding their sending in a system. For this reason, the TA initially chooses an extraordinary 1024-piece mystery number N for each CNj and the hub connected with CNj , and figures its pseudo personality utilizing its own character IDTA as RIDTA = h(IDTA||N). The TA at that point picks a novel character IDCNj for each CNj , and computes its relating pseudo personality RIDCNj = h(IDCNj ||N) and the brief accreditation of CNj utilizing its enlistment timestamp RTSCNj as TCCNj = h(IDTA ||RTSCNj ||N). The TA at last stores the data {RIDCNj , TCCNj , RIDTA} in the memory of CNj and sends it in the organization field.

For the pairwise key foundation between a sent CNj and hub in organize, we utilize the current polynomial-based key conveyance convention proposed by Blundo et al. [3]. For each CNj , the TA initially chooses a novel symmetric bivariate poly-nomial P(x, y) of degree n over a limited field (Galois field) GF(p). Note that the prime p is picked as a vast number and n is likewise substantial, which is significantly bigger than the quantity of number of hubs conveyed in a system appended with CNj to protect genuine security.

Once the hubs and CNj are conveyed, the principal undertaking of CNj and hub is to set up pairwise mystery keys utilizing the prestacked data put away in their directing table. Assume conveyed hubs and CNj need to build up a pairwise mystery key between them. Hub initially sends its pseudo personality RIDnode to CNj . In a comparative way, CNj likewise sends its pseudo personality RIDCNj to hub. After that hub processes the mystery key imparted to CNj utilizing its own particular polynomial offer as SKnode, CNj = P(RIDnode ,RIDCNj). Then again, CNj likewise processes a similar mystery key imparted to hubs utilizing its own polynomial offer as SKCNj, IMDl= P(RIDCNj, RIDnode) = P(RIDnode, RIDCNj) (=SKnode, CNj) since the polynomial P(x, y) is symmetric. Henceforth, both hub and CNj will convey safely utilizing the built up shared key SKnode,CNj. The proposed plot gives better security, enhance arrange throughput and furthermore demonstrates low end-to-end delay.

3. Security Analysis

MANETs are defenseless against different assaults. General assault composes are the dangers against Physical, MAC, and system layer which are the most vital layers that capacity for the steering instrument of the specially appointed system. Assaults in the system layer have by and large two purposes: not sending the bundles or including and changing a few parameters of steering messages. In this segment, we demonstrate that the proposed conspire is secure against the accompanying conceivable known assaults

Replay Attack: In the proposed conspire, amid the au-thentication and key understanding stages, the messages Msg1 = (M1,M2, T1), Msg2 = (M3, M4, T2) and Msg3 = (M5, T3) are traded between a client hub and hub CNj . These messages include diverse current timestamps T1, T2 and T3. On the off chance that a foe A captures these messages and endeavors to replay these messages later, the legitimacy of timestamps in these messages will fall flat, and subsequently, the messages will be dealt with as the old mes-sages. Subsequently, our plan gives assurance against replay assault.

Man-in-the-Middle Attack: Suppose A captures the message Msg1 and endeavors to change this message. For making the legitimate message, A can produce an irregular nonce R and current timestamp T. At that point, A can't process M' since he/she doesn't know RID'TA and k, which is the mystery key of hub. Along these lines, A can't alter Msg1. Additionally, A can't change different messages Msg2 and Msg3. Consequently, our plan gives insurance against man-in-the-center assault.

Blackhole assault: In blackhole assault, the vindictive hub sits tight for the colleagues to start a RREQ bundle. since the hub gets the RREQ parcel, it will promptly send a false RREP bundle with a changed higher grouping number. In this way, that the source hub expect that hub is having the crisp course towards the goal. The source hub overlooks the RREP bundle gained from different hubs and starts to send the measurements parcels over malignant hub. A malevolent hub takes the greater part of the courses toward itself. It doesn't allow sending any parcel anyplace.

Grayhole assault: The grayhole assault is a type of Denial of administration (DoS) assaults. in this assault, a foe first popular the indistinguishable conduct as a fair hub all through the way disclosure methodology, and after that quietly drops a couple or the greater part of the records parcels despatched to it for comparably sending regardless of whether no blockage happens. The perni-

cious hubs could corrupt the system perfor-mance; bother way disclosure procedure, et cetera.

Wormhole assault: The wormhole impact is caused by endeavors to attract all system activity to pernicious hubs that communicate counterfeit most limited way directing data. Wormhole assault is difficult to distinguish in light of the fact that this assault does not infuse irregular volumes of movement into the system. In a wormhole assault, aggressors "burrow" parcels to another zone of the system bypassing typical courses.

4. Result Analysis

In this section, to measure the impact of the projected theme on the network performance parameters, like end-to-end delay (in seconds) and throughput (in bits per second), we have used widely accepted NS2 2.34 simulator [37], [38] on Fedora 8 platform.

4.1 Simulation Parameters

The experimental simulation is implemented in the NS-2. The random waypoint model is selected as a mobility model in a rectangular field (1000 x 500 meters) with a nodes speed uniformly between 5 and a maximum value of 20 *m/s*.
Nodes remain stationary for a specified period called the "pause time". In the simulation work, we are considering the Ad hoc On Demand Distance Vector (AODV) protocol and Blackhole AODV protocol. The total simulation time is 100 seconds. In the simulations, we have varied two parameters node velocity and number of nodes in a given area. At a time, one variable was changed and other was kept constant. Apart from these, all other standard parameters are considered for the simulation.

4.2 Simulation Result

Keeping in mind the end goal to quantify the effect of the proposed system, we have computed the system execution parameters, similar to end-to-end postponement and throughput.

1) End-to-end Delay:
This metrics calculates the time into the packet bearing period at the source and the packet accomplishing period at the destination. Here salvo somebody information packet is lost or dropped at some point of the transmission, afterward such will not be viewed because of the same. Sometimes delay takes place because about discovery of route, queuing, intermediate link failure, packet retransmissions, etc., while calculating the delay. For such kind concerning metrics we have in conformity with measure in opposition to the distinct number regarding nodes, different traffic patterns and data connections.
The end-to-end delay of the proposed scheme for different scenarios is provided in Fig. 1. The values of end-to-end delay are decreasing with respect to time. Note that the value of end-to-end delay increases with the increasing number of nodes. The increment in number of nodes results more number of exchanged messages, which further incurs congestion, and therefore, end-to-end delay increases as number of nodes increase in network.

2) Throughput:
This metrics calculates the total number of packets delivered per second, means the quantity number of messages which are delivered per second. The network throughput (in bps) of the proposed scheme under different network scenarios is provided in Fig. 2. Note that the simulation time as 35s, which is considered as the total time. The throughput values increases with increase in time, and after some time interval it shows steady improvement.

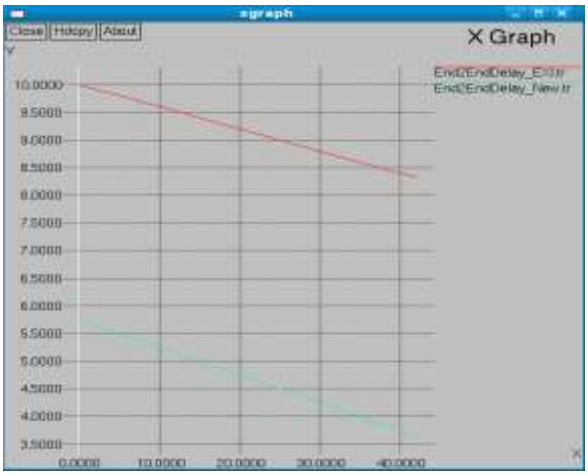

Figure 1:. Network performance: end-to-end delay

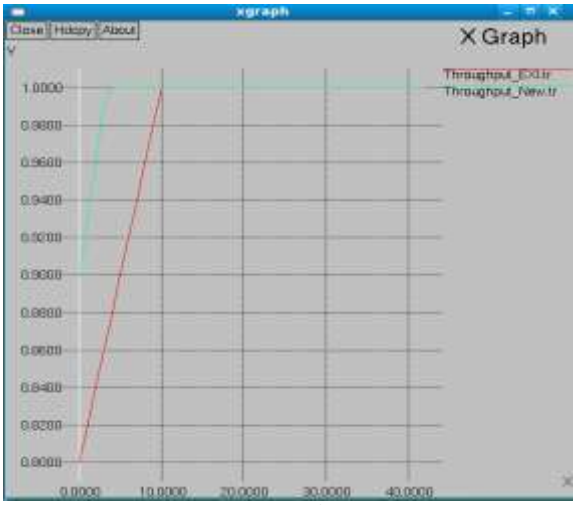

Figure 2:. Network performance: throughput

5. Conclusion

In this paper, we proposed a dynamic hub verification plot through which a hub and a controller hub can commonly validate each other and set up a session key for their future secure correspondence. Aside from that the pairwise key foundation between a controller hub and its neighbor hub is likewise given in the proposed plan to the safe correspondence between them. The calculation and correspondence expenses of the proposed conspire are tantamount with the current related plans. Moreover, the proposed plot additionally gives better security against various sort of assaults when contrasted with other existing related plans.

References

[1] Sudha Singh, S.C. Dutta, and D.K. Singh, "A study on Recent Research Trends in MANET" International Journal of Research and Reviews in Computer Science (IJRRCS)., Vol. 3, no. 3, pp. 1654–1658,. June 2012.
[2] Yih-Chun Hu, "Wormhole Attacks in Wireless Networks," IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS., vol. 24, no. 2, pp. 370 – 380 , . 2006.
[3] Ming Yu, Mengchu Zhou, "A Secure Routing Protocol against Byzantine Attacks for MANETs in Adversarial Environments," IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY., vol. 58, no. 1, pp. 449– 460,. 2009.
[4] Hidehisa Nakayama, "A Dynamic Anomaly Detection Scheme for AODV-Based Mobile Ad Hoc Networks," IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY., vol. 58, no. 5, pp. 2471 – 2481,. 2009.
[5] Majid Khabbazian, Hugues Mercier, and Vijay K. Bhargava, "Severity Analysis and Countermeasure for the Wormhole Attack in

Wireless Ad Hoc Networks," IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS., vol. 8 , no. 2 , pp. 736 – 745, . 2009.

[6] Bing Wu, Jianmin Chen, Jie Wu, Mihaela Cardei , "A Survey of Attacks and Countermeasures in Mobile Ad Hoc Networks," Wireless Network Security Signals and Communication Technology , pp 103-135., 2007

[7] Srdjan Capkun, "Integrity Regions: Authentication through Presence in Wireless Networks ," IEEE TRANSACTIONS ON MOBILE COMPUTING., vol. 9, no.11, pp. 1608–1621, . 2010.

[8] Karim El Defrawy, Gene Tsudik, "ALARM: Anonymous Location-Aided Routing in Suspicious MANETs," IEEE TRANSACTIONS ON MOBILE COMPUTING., vol. 10, no. 9, pp. 1345–1358,. 2011.

[9] Ying Xuan, Yilin Shen, Nam P. Nguyen, and My T. Thai , "A Trigger Identification Service for Defending Reactive Jammers in WSN," IEEE TRANSACTIONS ON MOBILE COMPUTING., vol. 11, no. 5, pp. 793–806, . 2012.

[10] Ziming Zhao, Hongxin Hu , "Risk-Aware Mitigation for MANET Routing Attacks," IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING., vol. 9, no. 2, pp. 250 – 260, . 2012.

[11] Elhadi M. Shakshuki, Nan Kang, "EAACK—A Secure Intrusion-Detection System for MANETs," IEEE TRANSACTIONS ON INDUSTRIAL ELECTRONICS., vol. 60, no. 3, pp. 1089–1098 , . 2013.

[12] Quansheng Guan, F. Richard Yu , "Joint Topology Control and Authentication Design in Mobile Ad Hoc Networks With Cooperative Communications," IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY ., vol. 61, no. 6, pp. 2674–2685, . 2012.

[13] Shiva Murthy G, Robert John D'Souza, and Golla Varaprasad, "Digital Signature-Based Secure Node Disjoint Multipath Routing Protocol for Wireless Sensor Networks," IEEE SENSORS JOURNAL ., vol. 12, no. 10, pp. 2941 –2949, . 2012.

[14] [14] Nikolay A. Moldovyan, "Blind Signature Protocols from Digital Signature Standards ," International Journal of Network Security ., vol. 13, no. 1, pp. 22–30, . 2011.

[15] BÃla_zej Brzezniak, Lucjan Hanzlik, "Attack against Ibrahim's Distributed Key Generation for RSA," International Journal of Network Security., vol. 15, no. 1, pp. 237–240, . 2013.

[16] Dae Hyun Yum, Jin Seok Kim, Sung Je Hong, "Distance Bounding Protocol for Mutual Authentication," IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS .,vol. 10, no. 2, pp. 592– 601,. 2011.

[17] KHABBAZIAN *et al.*, "Severity Analysis and Countermeasure for the Wormhole Attack in Wireless Ad Hoc Networks," IEEE TRANSACTIONS ON WIRELESS COMMUNICATION., vol. 8, no. 2, pp. 736–745, . 2009.

[18] H. Kim et al. , " Novel Defense Mechanism against Data Flooding Attacks in Wireless Ad Hoc Networks," IEEE Transactions on Consumer Electronics., vol. 56, no. 2, pp. 579–582, . 2010.

[19] Mike Burmester, Breno de Medeiros, "On the Security of Route Discovery in MANETs," IEEE TRANSACTIONS ON MOBILE COMPUTING., vol. 8, no. 9, pp. 1180 1188, . 2009.

[20] Mueen Uddin et al., " Signature-based Multi-Layer Distributed Intrusion Detection System using Mobile Agents", *International Journal of Network Security, Vol.15, No.2, PP.97-105, Mar. 2013*.

[21] Jie Yang, Yingying (Jennifer) Chen, "Detection and Localization of Multiple Spoofing Attackers in Wireless Networks," IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS ., vol. 24, no. 1, pp. 44–58, . 2013.

[22] Zhang Jianhong1, Xu Min2, and Liu Liying3, "On the Security of a Secure Batch Verification with Group Testing for VANET," International Journal of Network Security, Vol.16, No.5, PP.355–362, Sept. 2014.

[23] [23] CaLynna Sorrells1 and Lijun Qian2, "Quickest Detection of Denial-of-Service Attacks in Cognitive Wireless Networks", International Journal of Network Security, Vol.16, No.6, PP.468-476, Nov. 2014

[24] Radhika Goel, Anjali Sardana, and Ramesh C. Joshi, "Parallel Misuse and Anomaly Detection Model," *International Journal of Network Security*., vol. 14, no. 4, pp. 211–222, . 2012.

[25] [25] Jianbin Hu, Hu Xiong, and Zhong Chen , "Further Improvement of An Authentication Scheme with User Anonymity for Wireless Communications," *International Journal of Network Security* ., vol. 14, no. 5, pp. 297–300 , . 2012.

[26] Kavitha Ammayappan, Vinjamuri Narsimha Sastry, and Atul Negi , "A New Secure Route Discovery Protocol for MANETs to Prevent Hidden Channel Attacks," *International Journal of Network Security* ., vol. 14, no. 3, pp. 121–141, . 2012.

[27] Mina Malekzadeh, Abdul Azim Abdul Ghani, Shamala Subramaniam, and Jalil Desa, " Validating Reliability of OMNeT++ in Wireless Networks DoS Attacks: Simulation vs. Testbed," International Journal of Network Security., vol. 13 , no. 1 , pp. 13 – 21, . 2011.

[28] Kou-Min Cheng, Ting-Yi Chang, and Jung-Wen Lo, "Cryptanalysis of Security Enhancement for a Modified Authenticated Key Agreement Protocol," *International Journal of Network Security*,. vol. 11, no. 1, pp. 55–57, . 2010.

[29] M. Balakrishnan, H. Huang, R. Asorey-Cacheda , "Measures and Countermeasures for Null Frequency Jamming of On-Demand Routing Protocols in Wireless Ad Hoc Networks," IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS ., vol. 11, no. 11, pp. 3860–3868, .2012.

[30] Zhao Min, Zhou Jiliu, "Cooperative Black Hole Attack Prevention for Mobile Ad Hoc Networks", IEEE International Symposium on Information Engineering and Electronic Commerce, IEEE Xplore Press, 978-0-7695-3686-6/09, pp. 26-30, 2009.

[31] Jeba Veera Singh Jebadurai, Alfred Raja Melvin A, "Sinkhole Detection in Mobile Ad-hoc Networks Using Mutual Understanding among Nodes", IEEE International Conference on Electronics Computer Technology, IEEE Xplore Press , 978-1-4244-8679-3/11, pp. 321-324, 2011.

[32] Muhammad Zeshan, Shoab A.Khan, Ahmad Raza Cheema, Attique Ahmed, "Adding Security against Packet Dropping Attack in Mobile Ad hoc Networks", IEEE International Seminar on Future Information Technology and Management Engineering, IEEE Xplore Press 978-0-7695-3480-0/08, pp. 568-572, 2008.

[33] Venkat Balakrishnan, Vijay Varadharajan, and Uday Tupakula , "Mitigating Flooding Attacks in Mobile Ad-hoc Networks Supporting Anonymous Communications", IEEE International Conference on Wireless Broadband and Ultra Wideband Communications, IEEE Xplore Press 978-0-7695-2846-5/07, pp. 29, 2007.

[34] Aad, I., J.P. Hubaux, E.W. Knightly, "Impact of Denial of Service Attacks on Ad Hoc Networks", IEEE/ACM TRANSACTIONS ON NETWORKING., vol. 16, no. 4, PP. 791-802., 2008.

[35] Gao, X. and C. Wei, "A Novel Gray Hole Attack Detection Scheme for Mobile Ad-Hoc Networks". IEEE International Conference on IFIP Network and Parallel Computing Workshops, IEEE Xplore Press 978-0-7695-2943-1/07, pp: 209-2014,. 2007.

[36] Feng Li , "Attack and Flee: Game-Theory-Based Analysis on Interactions among Nodes in MANETs," IEEE TRANSACTIONS ON SYSTEMS, MAN, AND CYBERNETICS PART B: CYBERNETICS ., vol. 40, no. 3, pp. 612 – 622,. 2010.

[37] "The Network Simulator-ns-2," http://www.isi.edu/nsnam/ns/. Accessed on January 2017.

[38] J. Wang, "NS-2 Tutorial," http://www.cs.virginia.edu/ ˜cs757/slidespdf/ cs757-ns2-tutorial1.pdf. Accessed on April 2016.