Hybrid Trust-based Defense Mechanisms Against Sybil Attack in Vehicular Ad-hoc Networks

Agria Rhamdhan[1], Fadhil Hidayat[2]
{agria.rhamdhan@students.itb.ac.id[1], fadhil@stei.itb.ac.id[2]}

Institut Teknologi Bandung, Bandung, Indonesia[1,2]

Abstract. The application of IoT in Vehicular Ad-Hoc Networks (VANET) allows the realization of intelligent transportation systems to ensure the comfort and safety of road users. However, as an implication, attacks that can interfere with this aim certainly need to be a significant concern. It is because the stakes are not only network security but also the safety of the driver and its passengers. One of the attacks which had a substantial impact on VANET was the Sybil attack. Sybil attackers illegally change into several different identities to carry out malicious activities such as disrupting routing, causing traffic jams, bottlenecks, and even accidents. Various security methods are introduced to VANET to detect Sybil attacks, but there are still several issues that have not been resolved. In this paper, we proposed the design of a defense mechanism against Sybil attacks. This mechanism aims to be suitable for application on IoT networks that have limited resources an also considering accuracy, privacy, safety, and real-world implementations. The proposed design uses a hybrid scheme with a trust-based method. Each node has an obfuscated identity to guarantee privacy. The trust center in the form of a Road Side Unit (RSU) will give a reputation value to each identity that will be evaluated periodically when in the range. Nodes form a fully distributed network when there is no RSU. It will use a data-centric neighbor trust scheme where its neighbors will assess each node based on the exchanging data. Each node reports on suspicious nodes to the RSU for evaluation. This mechanism allows RSU to evaluate suspicious node, which decides to isolate that Sybil node out of network.

Keywords: Sybil Attack, VANET, Network Security, IDS

1 Introduction

Currently, the Vehicular Ad-Hoc Network (VANET) is an area of a research topic that is being widely discussed. With the existence of VANET, intelligent vehicles can communicate with each other (Vehicle to Vehicle / V2V communication) and with Roadside Infrastructure (Vehicle to Infrastructure / V2I communication). These two communications enable the realization of an intelligent transportation system to provide security, safety, and comfort to road users.

Following its purpose, the safety and security of the VANET are mandatory, because the stakes are not only the security system but also the driver and its passenger's lives. One of the significant attacks on VANET is a Sybil attack. Sybil attack is defined as an intrusion where malicious devices get or change into several different identities illegally, by forging or impersonating legitimate nodes. The objective is to disrupt the proper functioning of VANETs. This type of attack disguises itself as legitimate devices, and it is done by the

MSCEIS 2019, October 12, Bandung, Indonesia

DOI 10.4108/eai.12-10-2019.2296524

attacker camouflage its intrusion packet data is similar to regular data packets. Security systems would find it difficult to distinguish between the two types of data packages. Prior knowledge of Sybil's characteristics is needed to design a suitable defense mechanism.

Several defense mechanisms have been proposed to detect these Sybil attacks. In general, we group them into defense mechanisms based on Cryptography, Location verification based, Network Behavior-based, resource testing, and Trust-based. However, there are still several issues that cannot be resolved related to the accuracy, privacy, safety, and implementation in the real world. So this research was conducted to solve several problems related to Vanet that are still an open problem, including as follows. Accuracy issue is that the defense mechanism can detect Sybil at each phase, and it must be able to discover the large percentage of Sybil nodes in any properties [1]. Privacy issue is that most vehicle users hope that their identity information can be stored in VANET because they are afraid that their trip will leak with that identity [2]. Safety issue is that VANET does not allow a decrease in reputation after a severe traffic accident to prevent another attack, because damage to life and things in this attack cannot be repaired [3]. Real-world implementation issue is that The installation of such infrastructure nationally is challenging to achieve in the early stages of VANET. Even in the medium term, there may still be many places that are not covered by RSU[4].

This research aims to design a defense mechanism that can accurately detect Sybil attacks, and it is expected to discover all the properties of Sybil attacks and ensure all issues that have been mentioned are covered. The rest of this paper is organized as follows. Section 2 discusses Sybil attack properties to be addressed in the defense mechanism. Section 3 presents the classification of current defense mechanisms and its limitation. The proposed system and its goals are discussed in Section 4. Finally, in Section 5, we present some concluding remarks and future works.

2 Sybil Attack Defense Mechanism

Sybil attack is an intrusion with malicious devices trying to connect to legitimate networks using some illegally obtained identity. Some of the effects of the Sybil attack on several protocols are described in [5], including distributed storage, routing protocol, data collection system, voting system, and fair allocation of resources mechanism. Especially in Vanet, this attack has severely impacted, such as disrupting routing, causing traffic jams, bottlenecks, and even causing accidents.

To avoid the Sybil attack effects, defense mechanisms that can detect Sybil attacks accurately are needed. Mishra [1] classifies Sybil attacks based on nature and tasks carried out during this attack into three phases, namely the compromise, deployment, and launch phases. This property is significant to be considered in the design of defense mechanisms so that these defense mechanisms can recognize behavior and predict the likelihood of the actions of Sybil attackers appropriately.

Considering the characteristics of Sybil in defense mechanism design is vital to improving detection accuracy. We have reviewed several defense mechanisms from Sybil attacks on Wireless Ad-Hoc Networks. Table 1. showed the taxonomy of the detection mechanism of Sybil attack in VANETS. In applying these defense mechanisms to VANET, in Table 2 mentioned several weaknesses to be considered. These deficiencies should be addressed to enable defense mechanisms that can detect Sybil attacks accurately, thoroughly, and suitable for VANET.

Table 1. Defense Mechanism Taxonomy

Method	Reference
Cryptography Based	[3], [6]–[14]
Location-Based	[4], [15]–[35]
Node Behavior	[36]–[42]
Resource Testing	[43], [44]
Trust-Based	[45]–[50, 51]

Table 2. The weakness of each defense mechanism

Method	Weakness
Cryptography Based	– Cryptographic Hardware and software dependencies. – Low scalability when adding new points which can increase resource requirements exponentially. – High memory usage, computing, and communication overhead that is not suitable for limited resource networks – To ensure the network has secure keys and algorithms and high costs are needed for key generation and key distribution. – Detection time must be adjusted to the possibility of changes in network or node location – Compatibility issue with network types and routing protocols on IoT.
Location Verification Based	– Some methods are not suitable for use on VANET networks because the accuracy of the estimated location decreases due to rapid changes in network topology and node position changes. – The accuracy of the method depends on the environment interference, multipath fading, and shadowing caused inaccurate location estimation [52]. – This method is not enough if implemented as a single mechanism [4]. It will be challenging to detect nodes that can manipulate signal strength or decrypt conspiring nodes. – With increasing node density, it is possible when two or more honest nodes that have adjacent positions will be identified as Sybil nodes. – Possible privacy violations where identity is needed to send position information so that the route of movement of the node can be traced
Network Behavior	– Only detect Sybil nodes according to the context expected by the detection method, so that Sybil nodes with specialized knowledge can escape detection. – It usually requires specialized hardware that has a large capacity to collect and analyze data.
Resource Testing	– Exponential increase for each node addition. – Extensive power consumption due to the need to carry out testing at all times. – Assuming a single channel, attackers who have more than one channel can manipulate the results of resource testing. – Valid nodes that have resource problems due to DoS or conditions such as power blackouts, overloaded processors, and others can be considered Sybil nodes.
Trust-Based	– This method cannot detect if the Sybil node dominates the number of nodes in the process of determining the value of trust, so additional arrangements are needed to overcome this.

4 Proposed Defense Mechanism

4.1 System Model

The defense mechanism proposed in this study can be seen in Figure 1. The proposed design has adopted the concept of a hybrid scheme with a trust-based method. The phases of this method are explained as follows. Each node has an obfuscated identity to guarantee privacy with the ID-Based Privacy Preservation scheme. The trust center in the form of a Road Side Unit (RSU) will give a reputation value to each identity that will be evaluated periodically when in the range. Nodes form a fully distributed network when there is no RSU. It will use a data-centric neighbor trust scheme where its neighbors will assess each node based on the exchanging data. Each node reports on suspicious nodes to the RSU for evaluation. RSU to evaluate suspicious node, that has been reported. Then decides to isolate that Sybil node out of network.

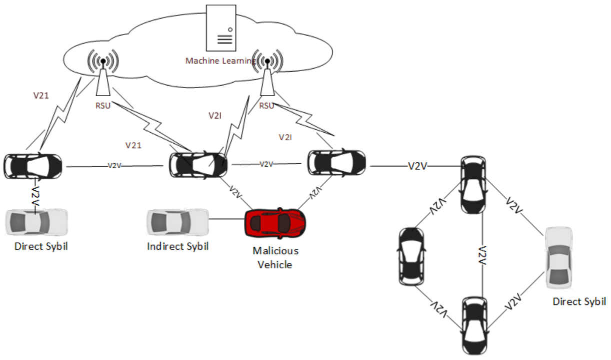

Fig. 1. System Model

4.2 Design Goal

The use of trust-based methods is used to allow the detection of individual nodes to increase the level of detection accuracy for each Sybil property. With reputation calculation, the RSU does not require detailed data related to identity, so together with an ID-based privacy preservation scheme, privacy and accuracy can be guaranteed.

In safety consideration, a detection system is implemented on a data-centric basis so that no nodes will be immediately ejected, for example, when there is misbehavior due to accidents and emergencies. It can prevent other accidents that result in the loss of both life and other material that cannot be repaired. By using a data-centric approach, trust is ensured on the information itself rather than on the information source [53], if there is a suspicious node then all nodes cooperatively provide a report to the RSU that will evaluate the suspicious node

Also, hybrid schemes are used, taking into account real-world implementation. So that although not all regions are covered nationally by the RSU, each node can still detect Sybil attacks with guaranteed privacy and safety.

For reputation calculations, each RSU will receive a report regarding a suspicious node from all nodes in its vicinity. The reputation value calculation is done using a machine learning-based reputation system by calculating the suspicious node report feedback received, including assessing whether the report is honest, dishonest, fake, or even incorrect because of a mistake. As an illustration, a comparison of defense mechanisms with previous research is shown in Table 3.

Table 3. Comparison of proposed defense mechanism

Parameter	Hamed, et al. [33]	Feng and Tang [3]	Yao, et al. [4]	Proposed Mechanism
Metode	Location-Based	Cryptographic based & Trust (event-based)	Location-based: RSSI Trust-based	Trusted Based (centralize: reputation/trust value & neighbor trust: data-centric/event-based)
Operation Topology	Centralized Vanet	Centralized Vanet	Decentralized Vanet	Hybrid Vanet
Lightweight	yes	no	yes	yes
Specialized Hw/Sw	RSU DMV GPS / DSRC	Trusted Authority RSU OBU Crypto Sw/Hw	no need	RSU OBU
Overhead	Communication: low Computation: low Memory: high (on RSU)	Communication: high Computation: high Memory: high	Communication: high Computation: low Memory: high	Prediction~Communication: low Computation: high (on RSU) Memory: low
Scalability	Poor	Poor	Good	Good
Mobility	yes	yes	yes	yes
Conspiracy Sybil	no	yes	no	yes
Fabrication/Stolen	both	Forge only	Forge only	both
Random/ selective	both	both	both	both
Simultaneous/non-simultaneous	non-simultaneous only	non-simultaneous only	both	both

5 Conclusion

In this paper, we propose the defense mechanism to address the accuracy, privacy, safety, and real-world implementation of issues in Sybil attack detection in VANET. The defense mechanism is based on a hybrid scheme with a trust-based method. RSU provides central trust by using a machine learning-based reputation system, and neighbor trust is run with a data-centric approach using message exchange. As future work, we plan to implement the proposed defense mechanism and to evaluate its detection accuracy and efficiency to detect the Sybil attack.

References

[1] A. K. Mishra, A. K. Tripathy, D. Puthal, and L. T. Yang, “Analytical Model for Sybil Attack Phases in Internet of Things,” *IEEE INTERNET OF THINGS JOURNAL*, vol. 6, no. 1, SI, pp. 379–387, Feb. 2019.

[2] X. Feng, C. Li, D. Chen, and J. Tang, “EBRS: Event Based Reputation System for Defensing Multi-source Sybil Attacks in VANET,” in *WASA*, 2015.

[3] X. Feng and J. Tang, “Obfuscated RSUs Vector Based Signature Scheme for Detecting Conspiracy Sybil Attack in VANETs,” *Mobile Information Systems*, vol. 2017, 2017.

[4] Y. Yao *et al.*, “Multi-Channel Based Sybil Attack Detection in Vehicular Ad Hoc Networks Using RSSI,” *IEEE Transactions on Mobile Computing*, vol. 18, no. 2, pp. 362–375, 2019.

[5] J. Newsome, E. Shi, D. Song, and A. Perrig, “The Sybil attack in sensor networks: analysis amp; defenses,” in *Third International Symposium on Information Processing in Sensor Networks, 2004. IPSN 2004*, 2004, pp. 259–268.

[6] K. M. Rabieh and M. A. Azer, “Combating sybil attacks in vehicular ad hoc networks,” *Communications in Computer and Information Science*, vol. 162 CCIS, pp. 65–72, 2011.

[7] R. Hussain and H. Oh, “On secure and privacy-aware sybil attack detection in vehicular communications,” *Wireless Personal Communications*, vol. 77, no. 4, pp. 2649–2673, 2014.

[8] T. Zhou, R. R. Choudhury, P. Ning, and K. Chakrabarty, “P2DAP - Sybil attacks detection in vehicular ad hoc networks,” *IEEE Journal on Selected Areas in Communications*, vol. 29, no. 3, pp. 582–594, 2011.

[9] N. Parikh and M. L. Das, “Privacy-preserving Services in VANET with Misbehavior Detection,” in *2017 IEEE International Conference on Advanced Networks and TELEcommunications Systems (Ants)*, 2017.

[10] A. S. Lal and R. Nair, “Region authority based collaborative scheme to detect Sybil attacks in VANET,” in *2015 International Conference on Control Communication Computing India (ICCC)*, 2015, pp. 664–668.

[11] M. Soni and A. Jain, “Secure Communication and Implementation Technique for Sybil Attack in Vehicular Ad-Hoc Networks,” in *Proceedings of the 2nd International Conference on Computing Methodologies and Communication, ICCMC 2018*, 2018, pp. 539–543.

[12] D. S. Reddy, V. Bapuji, A. Govardhan, and S. S. V. N. Sarma, “Sybil attack detection technique using session key certificate in vehicular ad hoc networks,” in *2017 International Conference on Algorithms, Methodology, Models and Applications in Emerging Technologies (ICAMMAET)*, 2017, pp. 1–5.

[13] M. Alimohammadi and A. A. Pouyan, “Sybil attack detection using a low cost short group signature in VANET,” in *2015 12th International Iranian Society of Cryptology Conference on Information Security and Cryptology (ISCISC)*, 2015, pp. 23–28.

[14] A. K. Sharma, S. K. Saroj, S. K. Chauhan, and S. K. Saini, “Sybil attack prevention and detection in vehicular ad hoc network,” in *2016 International Conference on Computing, Communication and Automation (ICCCA)*, 2016, pp. 594–599.

[15] K. M. Ali Alheeti, M. S. Al-ani, and K. McDonald-Maier, “A hierarchical detection method in external communication for self-driving vehicles based on TDMA,” *PLoS ONE*, vol. 13, no. 1, 2018.

[16] M. Ayaida, N. Messai, S. Najeh, and K. B. Ndjore, “A Macroscopic Traffic Model-based Approach for Sybil Attack Detection in VANETs,” *Ad Hoc Networks*, p. 101845, 2019.

[17] J. Grover, M. S. Gaur, and V. Laxmi, “A Novel Defense Mechanism Against Sybil Attacks in VANET,” in *Proceedings of the 3rd International Conference on Security of Information and Networks*, New York, NY, USA, 2010, pp. 249–255.

[18] T. M. De Sales, H. O. Almeida, A. Perkusich, L. De Sales, and M. De Sales, “A privacy-preserving authentication and Sybil detection protocol for vehicular ad hoc networks,” in *Digest of Technical Papers - IEEE International Conference on Consumer Electronics*, 2014, pp. 426–427.

[19] D. Jin and J. Song, “A Traffic Flow Theory Aided Physical Measurement-Based Sybil Nodes Detection Mechanism in Vehicular Ad-hoc Networks,” in *2014 IEEE/ACIS 13th International Conference on Computer and Information Science (ICIS)*, 2014, pp. 281–286.

[20] M. S. Mohamed, P. Dandekhya, and A. Krings, “Beyond passive detection of sybil attacks in VANET,” in *2017 6th International Conference on Reliability, Infocom Technologies and Optimization: Trends and Future Directions, ICRITO 2017*, 2018, vol. 2018-January, pp. 384–390.

[21] Y. Hao, J. Tang, and Y. Cheng, “Cooperative Sybil Attack Detection for Position Based Applications in Privacy Preserved VANETs,” in *2011 IEEE Global Telecommunications Conference - GLOBECOM 2011*, 2011, pp. 1–5.

[22] K. Lim, K. M. Tuladhar, and H. Kim, “Detecting Location Spoofing using ADAS sensors in VANETs,” in *2019 16th IEEE Annual Consumer Communications and Networking Conference, CCNC 2019*, 2019.

[23] B. Yu, C.-Z. Xu, and B. Xiao, “Detecting Sybil attacks in VANETs,” *Journal of Parallel and Distributed Computing*, vol. 73, no. 6, pp. 746–756, 2013.

[24] B. Płaczek and M. Bernas, “Detection of malicious data in vehicular ad Hoc networks for traffic signal control applications,” *Communications in Computer and Information Science*, vol. 608, pp. 72–82, 2016.

[25] C. Sowattana, W. Viriyasitavat, and A. Khurat, “Distributed consensus-based Sybil nodes detection in VANETs,” in *2017 14th International Joint Conference on Computer Science and Software Engineering (JCSSE)*, 2017, pp. 1–6.

[26] G. Yan, B. B. Bista, D. B. Rawat, and E. F. Shaner, “General active position detectors protect VANET security,” in *Proceedings - 2011 International Conference on Broadband and Wireless Computing, Communication and Applications, BWCCA 2011*, 2011, pp. 11–17.

[27] Z. A. Abdulkader, A. Abdullah, M. T. Abdullah, and Z. A. Zukarnain, “Malicious node identification routing and protection mechanism for vehicular ad-hoc network against various attacks,” *International Journal of Networking and Virtual Organisations*, vol. 19, no. 2–4, pp. 153–175, 2018.

[28] C. Iwendi, M. Uddin, J. A. Ansere, P. Nkurunziza, J. H. Anajemba, and A. K. Bashir, “On Detection of Sybil Attack in Large-Scale VANETs Using Spider-Monkey Technique,” *IEEE Access*, vol. 6, pp. 47258–47267, 2018.

[29] Y. Xin, X. Feng, and T.-T. Li, “Position related lightweight Sybil detection approach in VANET,” *Tongxin Xuebao/Journal on Communications*, vol. 38, no. 4, pp. 110–119, 2017.

[30] P. Vinoth Kumar and M. Maheshwari, “Prevention of Sybil attack and priority batch verification in VANETs,” in *2014 International Conference on Information Communication and Embedded Systems, ICICES 2014*, 2015.

[31] G. Yan, S. Olariu, and M. C. Weigle, “Providing VANET security through active position detection,” *COMPUTER COMMUNICATIONS*, vol. 31, no. 12, pp. 2883–2897, Jul. 2008.

[32] K. Selvakumar and S. Naveen Kumar, “Security issues and ANALYSING sybil attack detection in VANET,” *International Journal of Recent Technology and Engineering*, vol. 7, no. 5, pp. 386–391, 2019.

[33] H. Hamed, A. Keshavarz-Haddad, and S. G. Haghighi, “Sybil Attack Detection in Urban VANETs Based on RSU Support,” in *Electrical Engineering (ICEE), Iranian Conference on*, 2018, pp. 602–606.

[34] M. S. Bouassida, G. Guette, M. Shawky, and B. Ducourthial, “Sybil nodes detection based on received signal strength variations within VANET,” *International Journal of Network Security*, vol. 9, no. 1, pp. 22–33, 2009.

[35] Y. Yao *et al.*, “Voiceprint: A Novel Sybil Attack Detection Method Based on RSSI for VANETs,” in *2017 47th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, 2017, pp. 591–602.

[36] B. Subba, S. Biswas, and S. Karmakar, “A game theory based multi layered intrusion detection framework for VANET,” *Future Generation Computer Systems*, vol. 82, pp. 12–28, 2018.

[37] S. Han, D. Ban, W. Park, and M. Gerla, “Localization of Sybil Nodes with Electro-Acoustic Positioning in VANETs,” in *GLOBECOM 2017 - 2017 IEEE Global Communications Conference*, 2017, pp. 1–6.

[38] D. Gantsou, “On the use of security analytics for attack detection in vehicular ad hoc networks,” in *2015 International Conference on Cyber Security of Smart Cities, Industrial Control System and Communications, SSIC 2015 - Proceedings*, 2015.

[39] S. Ruj, M. A. Cavenaghi, Z. Huang, A. Nayak, and I. Stojmenovic, “On data-centric misbehavior detection in VANETs,” in *IEEE Vehicular Technology Conference*, 2011.

[40] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, “Performance comparison of reputation assessment techniques based on self-organizing maps in wireless sensor networks,” *Wireless Communications and Mobile Computing*, vol. 2017, 2017.

[41] R. Hussain, S. Kim, and H. Oh, “Privacy-aware VANET security: Putting data-centric misbehavior and sybil attack detection schemes into practice,” *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 7690 LNCS, pp. 296–311, 2012.

[42] S. Golestani Najafabadi, H. R. Naji, and A. Mahani, “Sybil attack Detection: Improving security of WSNs for smart power grid application,” in *Smart Grid Conference 2013, SGC 2013*, 2013, pp. 273–278.

[43] K. Rabieh, M. M. E. A. Mahmoud, T. N. Guo, and M. Younis, “Cross-layer scheme for detecting large-scale colluding Sybil attack in VANETs,” in *2015 IEEE International Conference on Communications (ICC)*, 2015, pp. 7298–7303.

[44] M. K. Saggi and R. Kaur, “Isolation of Sybil attack in VANET using neighboring information,” in *2015 IEEE International Advance Computing Conference (IACC)*, 2015, pp. 46–51.

[45] J. Grover, M. S. Gaur, V. Laxmi, and N. K. Prajapati, “A Sybil Attack Detection Approach Using Neighboring Vehicles in VANET,” in *Proceedings of the 4th International Conference on Security of Information and Networks*, New York, NY, USA, 2011, pp. 151–158.

[46] N. Bißmeyer, J. Njeukam, J. Petit, and K. M. Bayarou, “Central Misbehavior Evaluation for VANETs Based on Mobility Data Plausibility,” in *Proceedings of the Ninth ACM International Workshop on Vehicular Inter-networking, Systems, and Applications*, New York, NY, USA, 2012, pp. 73–82.

[47] S. Hamdan, A. Hudaib, and A. Awajan, “Hybrid Algorithm to Detect the Sybil Attacks in VANET,” in *2018 Fifth International Symposium On Innovation In Information And Communication Technology (ISIICT 2018)*, 2018, pp. 93–98.

[48] Y.-L. Shi and L.-M. Wang, “Spatio-Temporal Analysis Based Resist Conspiracy Sybil Attack Detection in VANETs [VANETs中基于时空分析的抗合谋Sybil攻击检测方法],” *Jisuanji Xuebao/Chinese Journal of Computers*, vol. 41, no. 9, pp. 2148–2161, 2018.

[49] C. Chen, W. Han, and X. Wang, “Sybil attack detection based on signature vectors in VANETs,” *International Journal of Critical Computer-Based Systems*, vol. 2, no. 1, pp. 25–37, 2011.

[50] J. Grover, V. Laxmi, and M. S. Gaur, “Sybil attack detection in VANET using neighboring vehicles,” *International Journal of Security and Networks*, vol. 9, no. 4, pp. 222–233, 2014.

[51] D. Airehrour, J. A. Gutierrez, and S. K. Ray, “SecTrust-RPL: A secure trust-aware RPL routing protocol for Internet of Things,” *Future Generation Computer Systems*, vol. 93, pp. 860–876, 2019.

[52] A. Vasudeva and M. Sood, “Survey on Sybil attack defense mechanisms in wireless ad hoc networks,” *Journal of Network and Computer Applications*, vol. 120, pp. 78–118, 2018.

[53] M. Raya, P. Papadimitratos, V. D. Gligor, and J. -. Hubaux, “On Data-Centric Trust Establishment in Ephemeral Ad Hoc Networks,” in *IEEE INFOCOM 2008 - The 27th Conference on Computer Communications*, 2008, pp. 1238–1246.