Innovative Systems Design and Engineering
ISSN 2222-1727 (Paper) ISSN 2222-2871 (Online)
Vol.11, No.4, 2020
www.iiste.org

# A Survey: Intrusion Detection System for Vehicular Ad-Hoc Networks (VANETs)

Kedir Lemma Arega
School of Technology and Informatics, Ambo University

**Abstract**
In recent years, the security issues on Vehicular ad hoc networks (VANETs) have become one of the primary concerns. Vehicular Ad Hoc Network has attracted both research and industrial community due to its benefits in facilitating human life and enhancing the security and comfort. However, various issues have been faced in such networks such as information security, routing reliability, dynamic high mobility of vehicles that influence the stability of communication. Furthermore, VANETs are vulnerable against attacks so this can directly lead to the corruption of networks and then possibly provoke big losses of time, money, and even lives. This paper presents a survey of VANETs attacks and solutions in carefully considering other similar works as well as updating new attacks and categorizing them into different classes.
**Keywords:** Intrusion Detection System
**DOI:** 10.7176/ISDE/11-4-02
**Publication date:**August 31st 2020

## 1. Introduction

Vehicular Ad-hoc Network (VANET) is not a new topic, it continues to provide new research challenges and problems[1]. It is a technology that uses moving cars as nodes in a network to create a mobile network[2]. The main objective of VANET is to help a group of vehicles to set up and maintain a communication network among them without using any central base station or any controller. A vehicle can communicate with another vehicle directly which is called Vehicle to Vehicle (V2V) communication, or a vehicle can communicate to an infrastructure such as a Road Side Unit (RSU), known as Vehicle-to-Infrastructure (V2I)[1].

VANETs introduce applications of Intelligent Transport System which provides legitimate information to the users on the road in order to increase the road and users safety. It is very effectively used for spontaneous creation of wireless network of vehicles for exchanging information between them, for improved transport and traffic management and to enable various users to be sufficiently informed about the road and make safer and smarter decisions on road by using transport networks [3].

With the development of VANET applications, there are so many issues raised. Among many other issues, security issue of VANET cannot be ignored. VANETs have wireless nature property, which makes it vulnerable for attackers to exploit. This opens the door for attackers to unconsciously or intentionally damage a part of or the total network. Attacks to VANETs may lead to catastrophic consequences such as the losses of lives in the case of traffic accident, losses of time (e.g., tampering traffic jam made by attacks) or financial losses (i.e., in payment services)[4].

## 2. Security Requirements in VANETs

Security in VANET is critical due to vulnerabilities exist during information transmission in VANET, which causing VANET exposed to the attacks. In order to maintain a secure vehicular communication and networks, VANET security system should satisfy with the requirements. Some of the requirements are essential for all networks, but some are definite for VANET only[5]. Those requirements are:

**2.1. Authentication**: in order to allow the communication between vehicles which sending and receiving information, VANET should authenticate each of them. This process may comprise the identification of the sender identity and the legitimacy of the sender to use the network[5]. Authenticity involves proof of identity. Users should be able to identify each other's identity with which they are interacting. It can be verified through authentication process so the unauthorized entity cannot participate in the communication.

**2.2. Availability:** is defined as the degree of the VANET system that must be operable and available when needed. A fast response time also must applicable for some applications[5].

**2.3. Privacy**: is one of the most important requirements in VANET. Privacy must ensure that the identity of the drivers and the location of the vehicles are not being exposed[5]. An attacker can easily intercept the message passing from sender to the receiver so that privacy can be leaked and content can be modified. So that secure message passing is required in VANET.

**2.4. Integrity**: the information exchange in between the sender and the receiver should be free from the alteration attacks. Thus, information can be trusted[5]. The message must not be altered in transit; it should be received at receiver node same as it is sent at sender node. Integrity guarantees that message has not been altered by unauthorized persons while in transmission.

**2.5. Non-repudiation**: it ensures that the origin of the information cannot be denying that it has sending the information[5]. Non-repudiation ensures that the sender and receiver cannot deny having sent and received the message respectively.

## 3. Attackers in VANET

**3.1. Passive Attackers:** As the name suggests these attackers do not participate in the communication process but only surveillance the wireless channel to bring out information and pass them to other attackers that is they have an indirect involvement in the attack [6].

**3.2. Active Attackers:** Active attackers have a direct involvement in the attack. These kinds of attackers either generate a wrong set of information or do not forward the correct information received that is the message is misinformed [6].

**3.3. Insider Attackers:** Such attackers are the legitimate users having complete knowledge of the configuration and usage of the network which provides them an easier access to creating problems as compared to other attack[6].

**3.4. Outsider Attackers:** As compared to the insider attackers these create fewer problems. Such intruders are the legitimate users and create problems by misusing the protocols of the network and thus attackers in such cases are limited[6].

**3.5. Malicious Attackers:** The objective of such attackers is to disturb the effective working of the network without drawing any personal benefits from it, but harming the network members and its function. Such attackers cause a severe damage to the network and are thus considered as the most hazardous[6].

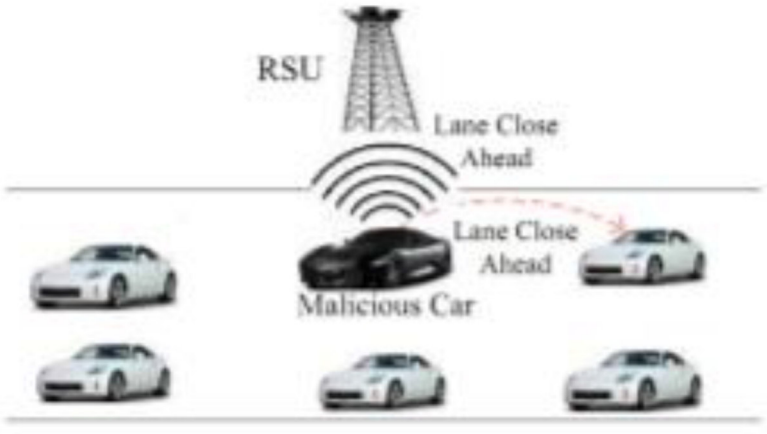
**3.6. Rational Attackers:** Being more predictable, such attackers seek to draw out personal benefits from the attack [6].

**3.7. Local Attackers:** Attackers are limited to a specified area and thus attack with a limited scope. But this may involve the main area of the road thus causing a severe damage in the network [6].

## 4. Attacks in VANET

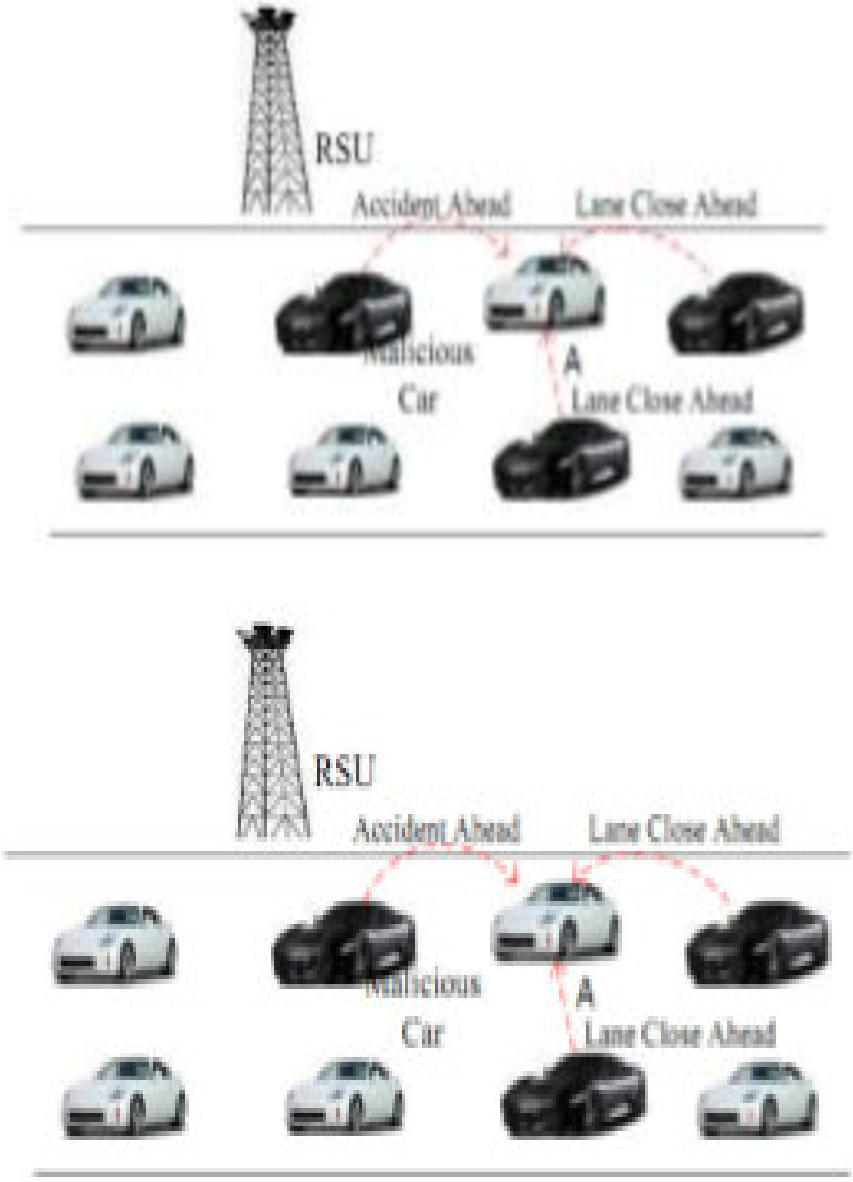
VANETs are exposed to various types of attacks both from internal and external. Attacks are mainly classified by two types inside and outside attacks. In an outside attack, the attacker is not a part of the network while in an inside attack, the attack can be initiated by compromised or malicious nodes that are part of the network. In the following, we discuss some potential cyber-attacks on VANET applications.

**4.1. Denial of Service (DoS) Attack:** is always one of the most serious level attacks in every network. The scenarios to perform are very diverse. The main aim is to prevent the authentic users to access the network services. In DoS attacks, attackers may transmit dummy messages to jam the channel and thus, reduce the efficiency and performance of the network. A part of or the total network is no longer available to legitimate users[4]. The below figure describe the concept of DoS.




**4.2. Distributed Denial of Service (DDos):** is more severe than the DoS where a number of malicious cars attack on a legitimate car in a distributed manner from different locations and timeslots. The below figure demonstrates that three malicious black cars attack on the car A from different locations and time so that A cannot communicate with the other vehicles[4].

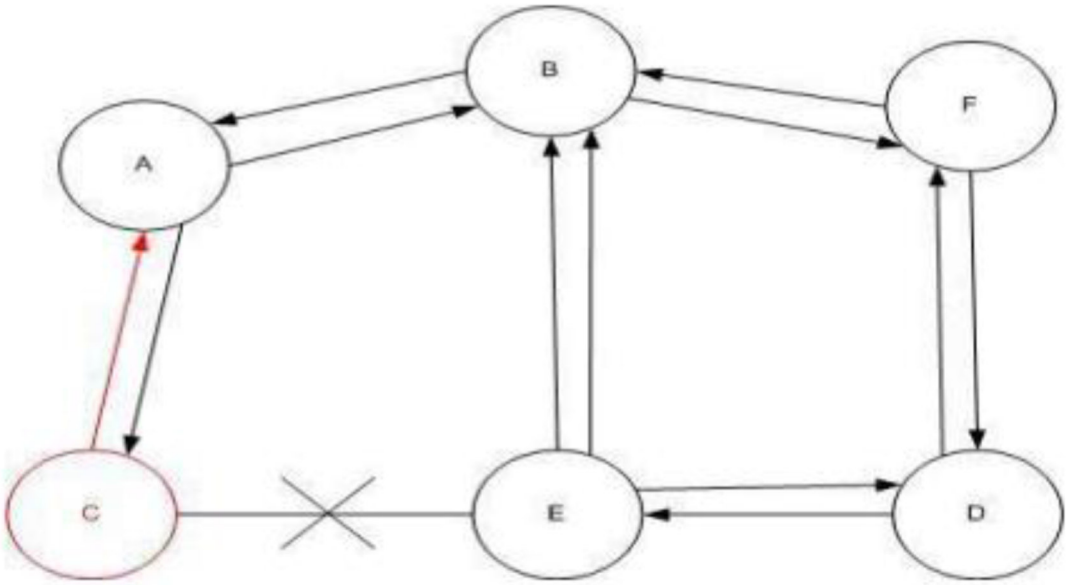
 




**4.3. Gray Hole attack:** This attack occurs if some node dropping 50% of the packets and rest 50% is sending by altering the message [6].

**4.4. Black hole attack:** is the attack that is carried out to disrupt the normal performance of the networks. It is a security attack in which malicious node absorbs all data packets by sending fake routing information and drops them without forwarding them. In black hole attack, a malicious node uses its routing protocol in order to advertise itself for having the shortest path to the destination node or to the packet it wants to intercept. Attacker node will always have the availability in replying to the route request and thus intercept the data packet and retain it. In protocol based on flooding, the malicious node reply will be received by the requesting node before the reception of reply from actual node; hence a malicious and forged route is created. When this route is establish, now it's up to the node whether to drop all the packets or forward it to the unknown address[7].




**4.5. Selective Forwarding Attack**: In this attack, malicious node acts as a normal node but it selectively drops some packets[8]. Black hole attack is the simplest form of selective forwarding attack in which all packets are dropped by the malicious node.

**4.6. Wormhole Attack:** In this attack, the adversary node creates a virtual tunnel between two ends. An adversary node acts as a forwarding node between two actual nodes. The two malicious nodes usually claim that they are one hop away from the base station. The wormhole attack can also be used to convince two distinct nodes that they are the neighbors by relaying packets between two of them [9].

**4.7. Sinkhole Attack:** In this attack, malicious node attracts network traffic towards it. To launch these types of attack, a malicious node attract all adjacent nodes to forward their packets through the malicious node by showing its routing cost minimum. The attacker creates an attack by introducing false node inside a network[8].

**4.8. Sybil Attack:** In this attack, the node has multiple identities. The routing protocol, detection algorithm and cooperation processes can be attacked by a malicious node[8].

**4.9. Hello Flood Attack:** In a sensor network, the routing protocol broadcast hello message to announce its presence to its neighbors. A node which receives the hello message may assume that the source node is within its communication range and add this source node to its neighbor list[10].

## 5. Intrusion detection system

Intrusion Detection System (IDS) is used to monitor the malicious traffic in particular node and network. It can act as a second line of defense which can defend the network from intruders. IDS can be a software or hardware tools. IDS can inspect and investigate machines and user actions, detect signatures of well-known attacks and identify malicious network activity. The goal of IDS is to observe the networks and nodes, detect various intrusions in the network, and alert the users after intrusions had been detected. The IDS works as an alarm or network observer it avoids damage of the systems by generating an alert before the attackers begin to attack. It can detect both internal and external attacks. Internal attacks are launched by malicious or compromised nodes that belong to the network, whereas external attacks are launched by third parties who are initiated by outside network [6].

IDS detect the network packets and determine whether they are intruders or legitimate users. There mainly three components of IDS: Monitoring, Analysis and detection, Alarm. The monitoring module monitors the network traffics, patterns and resources. Analysis and Detection is a core component of IDS which detects the intrusions according to specified algorithm. Alarm module raised an alarm if intrusion is detected [6].

**Types of intrusion detection systems**

1. **Signature Based IDS:** Signature based IDS matches the existing profile of the network against pre-defined attack patterns or signatures. It is also known as a rule-based detection technique. Signatures or patterns are pre-defined, stored in the database and each attack can be detected according to patterns or signatures. This technique is simple to use. This technique only requires patterns of individual attacks and must also store those patterns in some database. This approach needs specific knowledge of the individual attack. It needs more storage space with increasing the number of attacks. Thus, this approach is very expensive. This technique cannot identify new attacks unless their signatures or patterns are manually added into the database. So it needs up-gradation of database regularly with new signatures of attacks. Thus, it is a static approach. This approach has two main disadvantages: a) it needs the knowledge to form attack patterns. b) It cannot discover new and previously

unknown attacks [6].

2. **Anomaly Based IDS:** This technique is also known as event-based detection. This technique identifies malicious activities by analyzing the event. Firstly, it defines the normal behavior of the network. Then, if any activity differs from normal behavior then its mark as an intrusion. In this approach, a malicious node can be detected by matching the current protocol specification with previously defined protocol state. This approach detects attacks more efficiently than Signature based IDS. The main concepts behind this kind of security mechanisms are copied from statistical behavior modeling, which identifies malicious contents in a precise and reliable way with giving little incorrect positives rates. Automated training is generally used to define a normal behavior of the system. It is a very costly method for resource- constrained objects[6].

3. **Specification Based IDS:** This technique is somewhat similar to anomaly detection technique. In this technique, the normal behavior of the network is defined by manually, so it gives less incorrect positives rate. This technique attempts to excerpt best between signature-based and anomaly based detection approaches by trying to clarify deviations from normal behavioral patterns that are created neither by the training data nor by the machine learning method. The development of attack or protocol specification is done by manually so it takes more time. So, this can be a disadvantage of this approach[6].

**Existing IDS Approaches**

**Anomaly Based Approaches**

In[11], the authors proposed detection and interception of **Black Hole Attack** using Anomaly based approach. The paper was intended to present an effectual approach to detect and intercept this attack taking into account Dynamic MANET on-demand (DYMO) routing protocol. This work presupposes working in three modules- planting, detection and ultimately the interception against the black hole attack. An IDS is initiated on the notion of machine leaning using MATLAB software. A relative scrutiny of IDS grounded on classifiers like K-Nearest Neighbor, Support Vector Machine, Decision tree and neural network is also conducted to make it certain that the best feasible classifier is settled on for administering the IDS. The analysis of the put forward work is subsequently accomplished taking miscellaneous metrics covering packet drop rate, average transmission delay, Packet Delivery Ratio along with throughput.

**1. Specification Based approaches**

Chen Jun[12] proposed event processing based IDS to solve the problem of real time of IDS in VANET. In this approach, they designed the IDS architecture on the basis of Event Processing Model (EPM). It is rule-based IDS in which rules are stored in Rule Pattern Repository and takes SQL and EPL of Epser as a reference. According to obtained result, this approach consumed more CPU resources, consumed less memory and took less processing time than traditional IDS.

Ms. T. Eswari[13] proposed a rule-based intrusion detection system framework for VANET. There are three main phases of this approach. The first phase is local auditing phase which validates the packets to verify that packet is arriving from a valid neighboring node or not. The second phase is rule application phase which works in promiscuous mode. The third phase is intrusion detection phase which detects routing attacks by validating data collected from content suppression unit. This security mechanism can be able to detect only routing attacks.

In[14], the author analyze the effect of the wormhole attack in Optimized Link State routing (OLSR), which is a standard proactive routing protocol for VANET. A modified version of wormhole attack is developed in this paper, called camouflaging wormhole attack, and a corresponding specification based IDS is designed to detect and prevent this attack. Finally, Network Simulator (NS2) is used to measure the performance of the propose algorithm. The subsequent experimental results show that the efficiency of the proposed scheme.

**2. Cluster-Based Approach**

Christian Cervantes[15] proposed IDS to detect sinkhole attacks for VANET called as INTI which is implemented in Cooja simulator. The proposed system defines four modules. The first module is Cluster con- figure ration module which is responsible for classifying a node like members, leaders and associated according to their network functions. The second one is monitoring of routing module in which observer node monitors the number of transmissions is performed. The third one is attacker detection module which detects the sinkhole attacking node. The fourth module is the isolation of attacker module which isolates the malicious node from the cluster and it also raised an alarm to inform its neighboring nodes. The simulation result shows that 92% detection rate is achieved. This approach only detects sinkhole attacks so work can be enhanced by detection of other types of attacks.

**3. Hybrid Approach**

Shahid Raza[16] proposed a real-time intrusion detection system in IoT called as SVELTE. SVELTE is only IDS available in VANET which is implemented in Contiki OS. In this approach, there are three main centralized elements which are placed in 6LoWPAN Border Router. The first element is 6LoWPAN Mapped which collects information about the RPL protocol and rebuild the networks in 6BR. The second element is intrusion detection element which detects the intrusion by analyzing the mapped data. The third element is a distributed mini firewall which filters the malicious traffic before it reaches to the network. This approach can only detect spoofing attacks

inside the network, sinkhole and selective forwarding attacks.

## 6. Conclusion

In this paper, we made an attempt to provide a survey on the intrusion detection system for the VANET (vehicular ad-hoc network). With the development of VANET, there are so many issues raised. Among many other issues, security issues cannot be ignored. Here we discussed some potential security attacks which are made on VANET applications and various intrusion detection approaches which are available to mitigate those attacks. Still those approaches cannot be able to detect all types of cyber-attacks and are not feasible for VANET because it requires more processing power, memory and bandwidth for intrusion detection. Thus, future research in this direction would be to develop lightweight security mechanism which will take fewer resources for intrusion detection.

## References

[1] S. Rehman, M. A. Khan, T. A. Zia, and L. Zheng, "Vehicular Ad-Hoc Networks ( VANETs ) - An Overview and Challenges," *J. Wirel. Netw. Commun.*, no. May 2013, pp. 29–38, 2013.

[2] M. Kaur, S. Kaur, and G. Singh, "VEHICULAR AD HOC NETWORKS," *J. Glob. Res. Comput. Sci.*, vol. 3, no. 3, pp. 2010–2013, 2012.

[3] G. S. Chirayil and A. Thomas, "A Study on Cost Effectiveness and Security of VANET Technologies for Future Enhancement," *Procedia Technol.*, vol. 25, no. Raerest, pp. 356–363, 2016.

[4] V. H. La and A. Cavalli, "S ECURITY ATTACKS AND SOLUTIONS IN V EHICULAR A D HOC N ETWORKS : A S URVEY," *Int. J. AdHoc Netw. Syst.*, vol. 4, no. 2, pp. 1–20, 2014.

[5] M. Ali *et al.*, "Classification of Security Attacks in VANET : A Review of Requirements and Perspectives," *Int. J. Innov. Res. Comput. Commun. Eng.*, vol. 3, no. 3, March 2015, pp. 2339–2346, 2015.

[6] T. Sherasiya, H. Upadhyay, and H. B. Patel, "A SURVEY : INTRUSION DETECTION SYSTEM FOR INTERNET OF THINGS," *Int. J. Comput. Sci. Eng.*, vol. 5, no. 2, pp. 91–98, 2016.

[7] V. Bibhu, "Performance Analysis of Black Hole Attack in Vanet," *I. J. Comput. Netw. Inf. Secur.*, no. October, pp. 47–54, 2012.

[8] A. H. Farooqi and F. A. Khan, "A survey of intrusion detection systems for wireless sensor networks," *Int. J. Ad Hoc Ubiquitous Comput.*, vol. 9, no. 2, pp. 69–83, 2012.

[9] and R. S. Ismail Butun, Salvatore D. Morgera, "A Survey of Intrusion Detection Systems in Wireless Sensor Networks," *IEEE Commun. Surv. TUTORIALS*, vol. 16, no. 1, pp. 266–282, 1992.

[10] and K. M. Abdur Rahaman Sardar, Rashmi Ranjan Sahoo, Moutushi Singh, Souvik Sarkar, Jamuna Kanta Singh, "Intelligent Intrusion Detection System in Wireless Sensor Network," *Adv. Intell. Syst. Comput.*, vol. 2, pp. 707–712, 2015.

[11] S. H. Mahin, F. Taranum, L. N. Fatima, and K. U. R. Khan, "Detection and interception of black hole attack with justification using anomaly based intrusion detection system in MANETs," *Int. J. Recent Technol. Eng.*, vol. 8, no. 2 Special Issue 11, pp. 2392–2398, 2019.

[12] J. Chen and C. Chen, "Design of complex event-processing IDS in internet of things," *Proc. - 2014 6th Int. Conf. Meas. Technol. Mechatronics Autom. ICMTMA 2014*, pp. 226–229, 2014.

[13] A. H. Farooqi, F. A. Khan, J. Wang, and S. Lee, "A novel intrusion detection framework for wireless sensor networks," *Pers. Ubiquitous Comput.*, vol. 17, no. 5, pp. 907–919, 2013.

[14] C. B. Dutta and U. Biswas, "Specification based IDS for Camouflaging Wormhole Attack in OLSR," *23rd Mediterr. Conf. Control Autom.*, pp. 960–966, 2015.

[15] C. Cervantes, D. Poplade, M. Nogueira, and A. Santos, "Detection of sinkhole attacks for supporting secure routing on 6LoWPAN for Internet of Things," *Proc. 2015 IFIP/IEEE Int. Symp. Integr. Netw. Manag. IM 2015*, pp. 606–611, 2015.

[16] S. Raza, L. Wallgren, and T. Voigt, "SVELTE: Real-time intrusion detection in the Internet of Things," *Ad Hoc Networks*, vol. 11, no. 8, pp. 2661–2674, 2013.