A Review of Secured Message Transmission Techniques in VANET

A. PAVITHRA[1], DR. M. KOKILAMANI[2]

[1] *Department of Computer Science, Sree Saraswathi Thyagaraja College, Pollachi, Tamil Nadu, India*

[2] *Department of Computer Application, Kamalam College of Arts and Science, Anthiyur, Tamil Nadu, India*

Abstract- With the rapid advancement in the automotive industry, vehicles are now coming with equipped sensors, on board units and other processing as well communication capabilities. VANET have come into existence because of this advancement and has offered various research dimensions to the industry. VANET considered as a distinct type of Mobile Ad Hoc Networks, holds the opportunity to make people's life and death decisions by predicting and helping the drivers and other people about the road safety and other critical conditions. This paper outlines the VANET definition, its architecture, protocols, data dissemination strategies, attacks and application. Although, VANET are a subset of MANET but they are also the future of Intelligent Transport Systems. Such varied applications areas of VANET and future research directions of VANET are provided.

Indexed Terms- Ad-hoc networks, sensors, things, vehicular ad hoc networks, traffic information system, Denial of Service

I. INTRODUCTION

Vehicular ad-hoc networks (VANETs) are created by applying the principles of mobile ad hoc networks (MANETs) – the spontaneous creation of a wireless network of mobile devices – to the domain of vehicles. The concept of Vehicular Ad-hoc Networks (VANET) came into limelight which has opened new possibilities to avail the use of safety applications. VANET refers to a network created in an ad-hoc manner where different moving vehicles and other connecting devices come in contact over a wireless medium and exchange useful information to one another. The majority of VANETs applications require propagating messages in a very short time to all other vehicles within a range of few kilometers from the source. So efficient data dissemination is required to tackle the network partition and broadcast storm problems. In this article we will discuss about the applications, architecture and future of VANET. In this paper, we survey existing data dissemination techniques and their performance modeling approaches in VANETs, along with optimization strategies under two basic models: the push model, and the pull model.

1.1 CHARACTERIZATION OF VANET

VANET can be characterized by following factors:

- Dynamic topology

The speed and direction of vehicles changes constantly thereby resulting in high dynamic topology

- Intermittent connectivity

Connectivity between devices changes very frequently like connection between two devices exchanging information can disconnect anytime. The reason behind frequent disconnection is high dynamic topology.

- Mobility Patters

A large section of vehicles follow a certain patterns to move which is generally a function of traffic signals, speed limits, highways, streets, road conditions etc. These patterns when observed help in the creation of routing protocols for VANET

- Unlimited power and storage

It is assumed that the nodes in VANET are capable of possessing an unlimited amount of power as well as storage capacity. Therefore the nodes are free to exchange the data without the foundations of power consumption or storage wastage.

- On board sensors

VANET assumes that the nodes are seldom equipped with on board sensors which are capable of transmission of information to other devices or nodes. VANET also forms a very important part in Intelligent

Transport Systems as insights are produced from the information being exchanged by the vehicles and other devices in the VANET.

II. VANET ARCHITECTURE

VANET refers to a network created in an ad-hoc manner where different moving vehicles and other connecting devices come in contact over a wireless medium and exchange useful information to one another. A small network is created at the same moment with the vehicles and other devices behaving as nodes in the network.

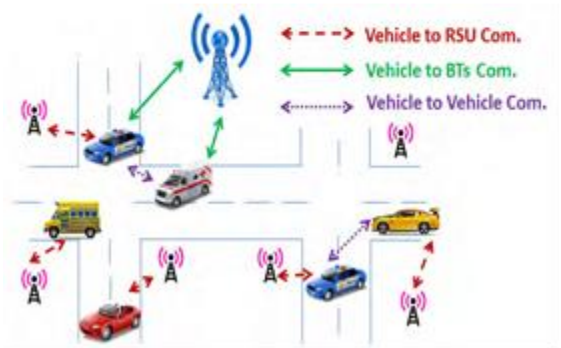

Figure 1: Architecture

Data dissemination in VANET depends upon three architectures:

- V2V: this is vehicle to vehicle architecture where vehicles act as both consumers and producers as vehicles receive information from other vehicles in the network and distribute that information to other vehicles in the network. So, both collection and distribution of data are done within the network for faster delivery of messages.

- V2I: This is vehicle to infrastructure wireless architecture in which infrastructure is used to collect information from vehicles and provide that information to other vehicles when necessary.

- Hybrid This is combination of both V2V and V2I architectures.

III. COMMUNICATION ARCHITECTURE

Another form of VANET architecture is communication architecture where communication types are characterized into 4 sections which are briefed as:

1) In vehicle communication: It detects the inner system data or performance of the vehicle and determines factors such as driver exhaustion or drowsiness etc. Determination of such factors and their extent is crucial for public safety as well as driver safety
2) Vehicle to Vehicle communication (V2V): The data exchange between different vehicles so as to assist the driver by informing them about warnings and other critical information to one another. V2V communication does not rely on fixed infrastructure for data exchange to happen and it helps in dissemination, safety and security applications.
3) Vehicle-to-road infrastructure (V2I) communication: This communication taking place between mobile vehicles and roadside fixed infrastructure in order to gather data. It provides updates related to environmental sensing and monitoring such as real time traffic update or weather update.
4) Vehicle-to-broadband cloud (V2B) communication: This allows communication of vehicles over broadband connections such as 3G/4G. This enhances the driver assistance and vehicle tracking as the broadband cloud may contain more of traffic information and other data. All the above listed communication types take place in a single or multiple VANETs.

The type of communication doesn't matter until and unless performance of VANET doesn't suffers. When vehicles move and an ad-hoc network is established, then information exchange begins. This transmission of information to other vehicles and nodes happen in one of the above listed ways.

The vehicle works and leverages the VANET as long as it stays in that particular network. VANET primarily supports two types of applications one is driver assistance and other is information dissemination. Driver assistance requires exchange of such information which assists the driver to maintain a more secure and efficient environment. Information dissemination focuses on delivering information to everyone such as drivers, nodes, passengers etc. Information dissemination applications range from critical safety applications to entertainment applications.

IV. PROTOCOLS FOR TRANSMISSION

The life of VANET lies in the communication that takes place between different vehicles. The data being gathered and exchanged by the vehicles requires some protocols or rules through which transmission can take place in a systematic and organized way. The data exchange between nodes in a VANET happens via routing protocols. These protocols define how a packet of data will be distributed among different nodes. On the basis of senders and receivers involved, three types of protocols are defined for VANET communications which are briefed as:

1) Unicast:
   Such protocols aim to deliver or transmit data from one source to one destination over a wireless medium. There are two ways to transmit packets; one is via multi-hop transmission where information of packet in transmitted further and further via hopping of packet to neighboring vehicle. Second one is carry and forward technique where a packet is carried by the vehicle as long as possible and then transmitted to reduce congestion or rebroadcast of packet. Third is trajectory based where nodes calculate various paths of data transmission and then transmit data by keeping in notice that minimum rebroadcast of packet happen?
2) Broadcast:
   Broadcasting protocols aim to deliver and communicate to as many nodes as possible. In situations like, road blocks, traffic jams, places with high traffic density or emergency situations, Broadcasting protocols are a must. They transmit data packet to more than one node at a time. On the counter side, broadcasting protocols also increase the chances of packet rebroadcast or storm Problem.

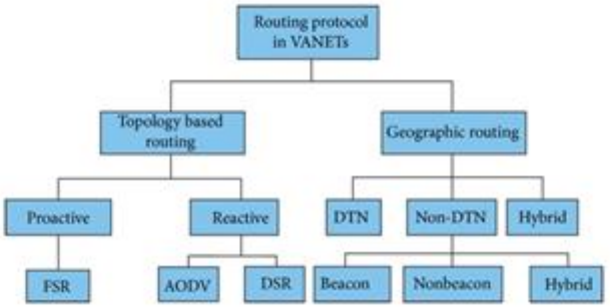

Figure 2: Protocols

V. DATA DISSEMINATION TECHNIQUES

Different data dissemination techniques for VANETs are proposed to fit different applications. Basically, two major applications are heavily researched in this area: traffic safety, and travel comfort. Traffic safety applications are low data-rate, confined to limited number of neighborhood with strict latency constraints.

While travel comfort applications are known as delay-tolerant applications with more relaxed time constraints, but are expected to require data transmission spanning relatively faraway distances.

5.1. Push model

Push model is generally preferred for safety messaging systems, such as collision warning systems, emergency message dissemination systems and information systems specified for hazardous road conditions like ice, water or snow. Nevertheless, other approaches also exist to support other types of applications such as arrival time estimation, speed expectation and congestion detection. In this section, a representative technique is provided for each of those applications.

5.2. Pull model

The pull model techniques often follow the request-response paradigm for data dissemination. Compared to the push-based model, pull model often requires less overhead, with less latency constraints. In pull-based approach, the requester usually sends a query to the broadcast site, and gets a reply message from there. In such applications, users can tolerate more delays as long as a response eventually returns. Pull-based techniques often target travel comfort applications such as service discovery and delay-tolerant systems.

VI. APPLICATIONS OF VANETS

The RSU can be treated as an access point or router or even a buffer point which can store data and provide data when needed. All data on the RSUs are uploaded or downloaded by vehicles. A classification of applications is also done by as Car to Car Traffic applications, Car to Infrastructure applications, Car to Home applications and Routing based applications. The authors in discusses about the various attacks based on their classification. Based on the type of communication either V2I or V2V, we are arranging the applications of VANETs into following classes:

1) Safety oriented,
2) Commercial oriented
3) Convenience oriented and
4) Productive Applications

6.1 Safety Applications

Safety applications include monitoring of the surrounding road, approaching vehicles, surface of the road, road curves etc. The Road safety applications can be classified as:

1) Real-time traffic: The real time traffic data can be stored at the RSU and can be available to the vehicles whenever and wherever needed. This can play an important role in solving the problems such as traffic jams, avoid congestions and in emergency alerts such as accidents etc.
2) Co-operative Message Transfer: Slow/Stopped Vehicle will exchange messages and co-operate to help other vehicles. Though reliability and latency would be of major concern, it may automate things like emergency braking to avoid potential accidents. Similarly, emergency electronic brake-light may be another application.
3) Post Crash Notification: A vehicle involved in an accident would broadcast warning messages about its position to trailing vehicles so that it can take decision with time in hand as well as to the highway patrol for tow away support
4) Road Hazard Control Notification: Cars notifying other cars about road having landslide or information regarding road feature notification due to road curve, sudden downhill etc.
5) Cooperative Collision Warning: Alerts two drivers potentially under crash route so that they can mend their ways
6) Traffic Vigilance: The cameras can be installed at the RSU that can work as input and act as the latest tool in low or zero tolerance campaign against driving offenses

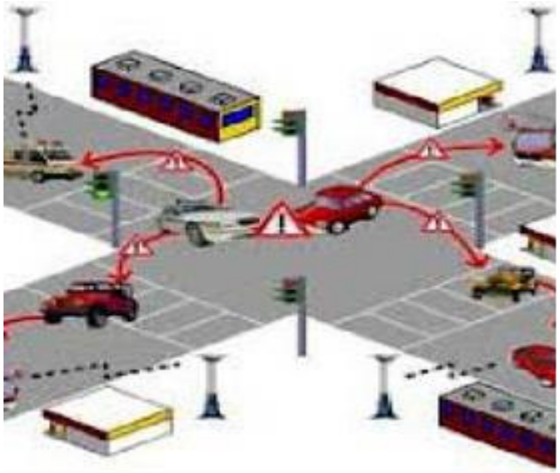

Figure 3: Real time traffic

6.2 Commercial Applications

Commercial applications will provide the driver with the entertainment and services as web access, streaming audio and video. The Commercial applications can be classified as:

1) Remote Vehicle Personalization/ Diagnostics: It helps in downloading of personalized vehicle settings or uploading of vehicle diagnostics from/to infrastructure.
2) Internet Access: Vehicles can access internet through RSU if RSU is working as a router.
3) Digital map downloading: Map of regions can be downloaded by the drivers as per the requirement before traveling to a new area for travel guidance. Also, Content Map Database Download acts as a portal for getting valuable information from mobile hot spots or home stations.
4) Real Time Video Relay: On-demand movie experience will not be confined to the constraints of the home and the driver can ask for real time video relay of his favorite movies
5) Value-added advertisement: This is especially for the service providers, who want to attract customers to their stores. Announcements like

petrol pumps, highways restaurants to announce their services to the drivers within communication range. This application can be available even in the absence of the Internet.

6.3 Convenience Applications

Convenience application mainly deals in traffic management with a goal to enhance traffic efficiency by boosting the degree of convenience for drivers. The Convenience applications can be classified as:

1) Route Diversions: Route and trip planning can be made in case of road congestions.
2) Electronic Toll Collection: Payment of the toll can be done electronically through a Toll Collection Point. A Toll collection Point shall be able to read the OBU of the vehicle. OBUs work via GPS and the on-board odometer or techograph as a back-up to determine how far the Lorries have travelled by reference to a digital map and GSM to authorize the payment of the toll via a wireless link. TOLL application is beneficial not only to drivers but also to toll operators.
3) Parking Availability: Notifications regarding the availability of parking in the metropolitan cities helps to find the availability of slots in parking lots in a certain geographical area. 4) Active Prediction: It anticipates the upcoming topography of the road, which is expected to optimize fuel usage by adjusting the cruising speed before starting a descent or an ascent. Secondly, the driver is also assisted.

Figure 4: Electronic toll collection

VII. ATTACKS IN VANET

Once the security requirements have been established for VANETs, many attacks can be identified to compromise them. In this section an elaborate discussion is made on these attacks, explaining how they can be performed and their potential consequences. For the sake of clarity, attacks have been classified depending on the main affected requirement.

7.1 Attacks on Identification and Authentication

- Impersonation is the case where an attacker pretends to be another entity. It can be performed by stealing other entity´s credential. As a consequence, some warnings sent to (or received by) a specific entity would be sent to (or received by) an undesired one.

- False attribute possession is a subtype of impersonation, in which the attacker tries to show the possession of an attribute (e.g. to be a member of an enterprise) to get some benefit. It could be performed if false credentials could be built, or if revoked credentials could be used normally. As a consequence, a regular vehicle could send messages claiming to be a police patrol, letting it to have a freeway.

- Sybil attacker uses different identities at the same time. In this way, a single vehicle could report the existence of a false bottleneck. Sybil attacks have been regarded as serious security threat to ad hoc and sensor networks. They impair the potential applications of VANETs by creating an illusion of traffic congestion. In the opinion of researchers, VANETs are facing a number of security threats, which impairs the efficiency of many VANETs potential applications and poses threat to even life safety. In Sybil attack a malicious vehicle claims to be at multiple locations with multiple identities thereby creating an illusion of traffic congestion. The malicious node can even spoil the proper functioning of the network by injecting false information.

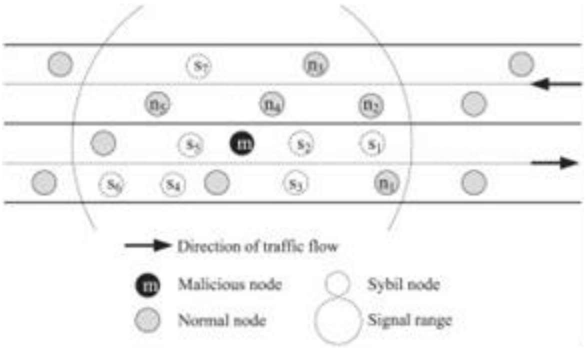

Figure 5: Sybil attack

Generally, in Sybil attack, a malicious node illegitimately takes on multiple identities. In mobile networking, each node gets the information of the neighboring node by receiving periodic beacons from neighbors in which they claim their identity. A malicious vehicle can manage to get identities of other vehicle by non-technical means such as stealing or it can also borrow from its friends. In the above Figure 5 the

Malicious node M creates an illusion of traffic congestion by claiming multiple identities thereby convincing other vehicles that there is a traffic jam and makes them to choose alternate route so that he makes his path clear. As presented in the VANET model, TPMs mounted on vehicles can store sensitive information like identifiers. In this way, the Sybil threat is alleviated. However, security mechanisms must be designed to provide identification and authentication, thus protecting against impersonation attacks.

7.2 Attacks on Privacy

Attacks on privacy over VANETs are mainly related to illegally getting sensitive information about vehicles. As there is a relation between a vehicle and its driver, getting some data about a given vehicle´s circumstances could affect its driver privacy. These attacks can then be classified attending to the data at risk:

- Identity revealing is a condition of getting the owner´s identity of a given vehicle that could put its privacy at risk. Usually, it is assumed that, a vehicle´s owner is also its driver, so it would simplify getting personal data about that person.
- Location tracking is also a privacy attack. The location of a vehicle in a given moment, or the path followed along a period of time are considered as personal data. It allows building that vehicle´s profile and, therefore, that of its driver. Mechanisms for facing both attacks are required in VANETs. They must satisfy the tradeoff between privacy and utility. In this way, security mechanisms should prevent unauthorized disclosures of information, but applications should have enough data to work properly.

7.3 Attacks on Non-Repudiation

The main threat related to non-repudiation is denying some action by some of the implicated entities. Non-repudiation can be circumvented if two or more entities share the same credentials. This attack is different from the impersonation attack described before – in this case, two or more entities collude to have a common credential. In this way, they get indistinguishable, so their actions can be repudiated. Credential issuance and management should be secured in VANETs to alleviate this threat. Although reliable storage has been assumed in vehicles (by their TPMs), having identical credentials in different vehicles should be avoided. Moreover, mechanisms that provide a proof of participation have to be also implemented.

7.4 Attacks on Confidentiality

- Eavesdropping is the most prominent attack over VANETs against confidentiality. To perform it, attackers can be located in a vehicle (stopped or in movement) or in a false RSU. Their goal is to illegally get access to confidential data. As confidentiality is needed in group communications, mechanisms should be established to protect such scenarios.

7.5 Attacks on Availability

As any other communication network, availability in VANETs should be assured both in the communication channel and in participating nodes. A classification of these attacks, according to their target, is as follows:

- Network Denial of Service (DoS): It overloads the communication channel or makes its use difficult (e.g. interferences). It could be performed by compromising enough RSUs, or by making a vehicle to broadcast infinite messages in a period of time.

- Routing Anomalies, is a particular case of network attacks that could lead to DoS. In this case, attackers do not participate correctly in message routing over the network. They drop all received messages (sinkhole attack) or just a few ones according with their interests (selfish behavior).
- Computation DoS overloads the computation capabilities of a given vehicle. Forcing a vehicle to execute hard operations, or to store too much information, could lead to this attack.

7.6 Attacks on Data Trust

Data trust can be compromised in many different ways in VANETs. Inaccurate data calculation and sending affects message reliability, as they do not reflect the reality. This could be performed by manipulating in-vehicle sensors, or by altering the sent information. Imagine that a vehicle reports an accident in road NH-7, while it really took place in NH-9. Such information should compromise such messages´ trust.

Even worse, sending false warnings (e.g. the accident didn´t take place) would also affect the whole system reliability. In this way, mechanisms to protect against such inappropriate data should be put in practice in vehicular contexts.

7.7 Authentication Scheme in VANET

The scenario for VANET communication includes communicating entities of the service providers (SP), the cars, and the access points (AP) operated on behalf of service providers. The SPs and the APs can communicate with each other by some application-layer proprietary protocols via Internet. The APs are deployed along the roadside with reasonable wireless coverage to facilitate communication. A car typically belongs to one wireless network service provider, and communicates with the APs for accessing the internet along the road it travels through. When it travels, it also roams into wireless coverage that provide by other authorities. To make the authentication process time-efficient, traditional solutions using centralized Authentication Server (AS) is not preferable because of the large amount of messages exchanged among the cars, the APs and the ASs. If the overlay network interconnecting the APs and the Ass is based on Internet, the delay for exchanging authentication messages could be prohibitive given the shortness of communication duration between the fast moving car and an individual AP.

Thus the authentication protocols are devised such that after the car initiates communication requests until the communication session is established, the protocol should involve as less parties as possible besides the car and the AP, and as less on demand communication over Internet as possible besides the wireless link between the two communicating parties. In addition, the number of messages exchanged in order for authentication should be controlled. In the design, the user authentication will be performed at the APs, i.e., the user will prove to the AP that it is a legitimate one. A more strict security will require the AP to prove it as a legitimate one as well, so to have mutual authentication. During the authentication, the two parties will negotiate a secret session key for the communication afterwards. The session keys could be established in a way that synchronizes the update at both the car and the AP so to allow location privacy counter measures.

7.8 Security Aspects Restricted to VANET

Generally, attacks cause anomalies to the network functionality. A lot of previous studies have investigated security vulnerabilities of routing protocols for wireless networks. Also, there are attacks in which malicious nodes advertise fake locations to their neighbor nodes.

- Position verification techniques to thwart position spoofing attacks.
- Traceability by trusted network authorities (e.g., network administrator) for privilege revocation once misbehavior is detected.
- Identity and location privacy preserving mechanisms against unlawful tracing and user profiling.
- Non-frame ability of an honest user, who cannot be falsely accused of having misbehaved.
- Detecting and correcting malicious data to ensure data consistency.
- The system must have light overheads in terms of computational costs and high efficiency.
- Preventing impersonation attacks, that is, no one can impersonate another authorized member to

cause service abuse problems and to damage the security of VANETs.

- Preventing eavesdropping, in other words, an intruder cannot discover some valuable information from communications between members in VANETs.
- Malicious attackers may damage the network by announcing fake node locations. Such attacks are even more difficult to mitigate.

7.9 Privacy Challenges

During a long-distance trip in high speed, a vehicular user could roam across multiple APs either belonging to their home wireless domain or to domains owned by different authorities including various service providers. This poses challenges on privacy and network performance to the current public wireless networks access protocols. The privacy challenge comes from traffic logging at AP's and at home domain in current public wireless LAN roaming protocols.

As a result, home and visited networks can acquire much personal information, e.g., the home network knows the current location of a mobile user, and the visited network knows the mobile user's identity and its home domain. Privacy in vehicular networks has to deal with threats that try to correlate received identifiers, or to correlate them to real-world identity, or to have position-identifier pairs. The performance challenge originates from the exchange of authentication messages between a user and its home domain when roaming. Mobile wireless communication has introduced new Location Privacy issue. Location Privacy is defined as an identity not being associated with a location, or a series of locations.

VIII. CONCLUSION

Vehicular Ad-hoc Network (VANET) is a vast and emerging area of research in vehicular communication technology. VANET is an infrastructure less network. It is utilized for upgrade in safety regarding applications and ease while during driving. VANET interfaces vehicles to share secure data during travelling on highways or roadways. The VANET applications are being developed for urban areas over the entire world. VANET provides an identity recognize system that has high effect in upgrade of activity administrations and overcoming the accidents on road. The major goal of this technology is to assemble a vehicle safety and security environment. There are so many architectures, algorithms and protocols and implementation have been made in current years to enhance the performance of vehicles during travelling. This paper outlines the basic overview of what a VANET, its application, protocols, data dissemination and so on. Further sections elaborate the architecture of VANET from system and communication point of view used by VANET. There are many advanced protocols developed nowadays. And in future my work deals with data dissemination and its delay which helps us to understand the safety message transmission.

REFERENCES

[1] Liang, W., Li, Z., Zhang, H., Wang, S., & Bie, R. (2015). Vehicular ad hoc networks: architectures, research issues, Methodologies, challenges, and trends. International Journal of Distributed Sensor Networks, 2015, 17.

[2] Bako, B., & Weber, M. (2011). Efficient information dissemination in VANETs. INTECH Open Access Publisher.

[3] Ranjan, P., & Ahirwar, K. K. (2011, January). Comparative study of vanet and manet routing protocols. In Proceedings of The International Conference on Advanced computing and communication Technologies (ACCT 2011).

[4] Kumar, R., & Dave, M. (2012). A review of various vanet data dissemination protocols. International Journal of u-and e-Service, Science and Technology, 5(3), 27-44.

[5] Da Cunha, F. D., Boukerche, A., Villas, L., Viana, A. C., & Loureiro, A. A. (2014). Data communication in VANETs: a Survey, challenges and applications (Doctoral dissertation, INRIA Saclay).

[6] Hartenstein, H., & Laberteaux, K. P. (2008). A tutorial survey on vehicular ad hoc networks. Communications Magazine, IEEE, 46(6), 164-171.

[7] Willke, T. L., Tientrakool, P., & Maxemchuk, N. F. (2009). A survey of inter-vehicle

communication protocols and their Applications. Communications Surveys & Tutorials, IEEE, 11(2), 3-20.

[8] Altayeb, M., & Mahgoub, I. (2013). A survey of vehicular ad hoc networks routing protocols. International Journal of Innovation and Applied Studies,3(3), 829-846.

[9] Panichpapiboon, S., & Pattara-Atikom, W. (2012). A review of information dissemination protocols for vehicular ad hoc networks. Communications Surveys & Tutorials, IEEE, 14(3), 784-798.