Securing the Information in Social Media with STB Routing Protocol

Ms.S.Induja[1] Mr.P.Rajendran[2]
[1]PG Student [2]Assistant Professor
[1,2]Department of Computer Science and Engineering
[1,2]Selvam College of Technology, Namakkal Tamil Nadu, India

Abstract— With the proliferation of fairly powerful mobile devices and ubiquitous wireless technology, traditional mobile ad hoc networks (MANETs) now migrate into a new era of service-oriented MANETs where in a node can provide and receive service from other nodes it encounters and interacts with. This proposed research concerns trust management and its applications for service-oriented. MANETs to answer the challenges of MANET environments, including no centralized authority, dynamically changing topology, limited bandwidth and battery power, limited observations, unreliable communication, and the presence of malicious nodes who act to break the system functionality as well as selfish nodes who act to maximize their own gain. A context-aware trust management model called secure trust based (STB) routing protocol for service-oriented ad hoc networks is proposed in the proposed system. The novelty of the design lies in the use of trust calculation to dynamically estimate trustworthiness of a service provider based on its service behavior patterns in a context environment, treating channel conditions, node status, service payoff, and social disposition as "context" information. This develops a recommendation filtering mechanism to effectively screen out false recommendations even in extremely hostile environments in which the majority recommenders are malicious. This demonstrated desirable convergence, accuracy, and resiliency properties of STB.

Keywords: Social Media, STB Routing Protocol

I. INTRODUCTION

Currently wireless networks have grown significantly in the field of telecommunication networks. Wireless networks have the main characteristic of providing access of information without considering the geographical and the topological attributes of a user. Over the past few years, the wireless network has almost exploded due to the rapid development of the Internet, and also the growth of small mobile devices as an instrument of communication and data exchange. The most used today is a wireless network built on top of a wired network. The wireless nodes are able to act as bridges in a wired network called base-stations. An example of this wireless network is the cellular phone networks where a phone connects to the base-station with the best signal quality. The movement of the mobile devices is facilitated by moving communication cells from one base-station to another base-station. The main infrastructure requires a complex administrative work. The proposed system aim to provide secure and trust based routing scheme for MANET.

A. Service Oriented MANET (SOMANET)

With the proliferation of fairly powerful mobile devices and ubiquitous wireless technology, traditional mobile ad hoc networks (MANETs) now migrate into a new era of service-oriented MANETs wherein a mobile device can provide and receive service from other mobile devices it encounters and interacts with. A service-oriented mobile ad hoc network (MANET) is populated with service providers (SPs) and service requesters (SRs). A realization of service-oriented MANETs is a peer-to-peer service system with SPs providing web services and SRs requesting services, each requiring dynamic service composition and binding. Unlike a traditional web service system in which nodes are connected to the Internet, nodes in service-oriented MANETs are mobile and an SR will need to request services from available SPs it encounters and with which it interacts dynamically. One can view a service-oriented MANET as an instance of Internet of Things (IoT) systems with a wide range of mobile applications including smart city, smart tourism, smart car, smart environmental monitoring, and healthcare.

B. Wireless Attack Categories

The proposed work concentrates on intentional attacks upon the infrastructure of all-optical networks. By an "attack", we mean an action performed on the infrastructure of an all optical networks with an intention to disrupt network services and/or obtain unauthorized information. There exist several methods of attacks upon the infrastructure of all-optical networks. However, these attacks can be grouped into two categories for the purpose of attack detection.

1) Black Hole Attack

The black hole attack is network layer attack, all the packets are dropped by the hostile node and fake packets are further send for communication. In this the selfish or hostile node with the help of its routing protocol announces that it has the shortest path to destination. All the nodes in the network get this information then every node will start sending packets to this malicious/hostile node and after receiving all the packets, malicious node will simply drop all the packets and send fake packets.

Malicious node waits for the neighbors to initiate a RREQ packet. As the node receives the RREQ packet, it will immediately send a false RREP packet with a modified higher sequence number. So, that the source node assumes that node is having the fresh route towards the destination. The source node ignores the RREP packet received from other nodes and starts sending data packets to malicious node. A malicious node takes all the routes towards itself. It does not allow forwarding any packet anywhere. This attack is called a blackhole as it swallows all the data packets.

2) Eavesdropping Attack

Eavesdropping refers to the attempts of an attacker trying to obtain unauthorized information from an optical network. For example, an attacker can obtain the desired information by "tapping", which refers to the method of bending the fiber to change an incidence angle and allowing light to escape from a fiber core. Alternatively, an eavesdropper can

obtain the desired information from a "crosstalk channel", which refers to an adjacent output link (leaving from the network node shared by a legitimate light path) that contains portions of legitimate data signals as a result of component crosstalk at the network node.

3) Wormhole Attack

The wormhole attack belongs to network layer and it one of the most dangerous attack. It basically records information or traffic form one point, tunnels it and then broadcast it to other point. Packet Leases is one of the technique by which wormhole attack can be detected, Packet Leases can be geographic or temporal, and the reason of using leases method is that it will put a limit on greatest amount of transmission distance of a packet. With the help of some of some techniques wormhole techniques can be created for example packet encapsulation, high power transmission capability, packet relay, protocol distortion etc.

4) Grey Hole Attack

Grey hole attack or selective forwarding attack is an active, data traffic, insider, routing layer attack. It can be a serious threat to data sensitive applications like health care and fire monitoring, Classified E-mails etc. A grey hole node is one which could start behaving as a black hole node from time to time i.e. It can behave like an attacker and drop the packets. So, It can be seen as a variation on black hole attack. In wireless mesh networks. Thus, detecting a grey hole attack is more complex and needs in depth studies.

The grey hole attack takes place in two phases-

- In first phase, A malicious node advertises itself as having an optimal path to the destination with the intentions of capturing the packets on that route
- In second phase, malicious node starts dropping packet on that route. After dropping some packets the node starts behaving normally again. Due to This behavior of it is difficult to detect malicious behavior in the network.

II. DETAILS OF METHODOLOGY

A. Existing System

The nature of MANETs brings a plethora of security challenges that need to be addressed. The vulnerability of communication channels and nodes and the high mobility of the changing topology make the security of MANETs difficult to deal with. The wireless broadcast of messages and the injection of false information in the network allow eavesdropping to happen thereby compromising the confidentiality and integrity of the whole network [4]. Different countermeasures, such as, cryptographic or trust-based approaches are proposed by the research fraternity to secure routing protocols in MANETs. While, cryptographic approaches are able to prevent tampering of routing information, they cannot secure the nodes participating in routing. On the other hand, trust-based mechanisms are able to not only secure the nodes but also the transmission of data. Traditional MANET routing protocols like AODV and FSR are susceptible to a number of security attacks, which include, black hole and grey hole attacks, flooding and Sybil attacks.

1) Drawbacks in Existing System

Grade Trust method doesn't detecting and isolating additional routing attacks such as: grey hole, worm hole, byzantine and flooding attack.

In FSR (Fisheye State Routing), nodes doesn't exchange link state data specifically with their neighbours to maintain the current topology information.

Secure trust level routing entails the development of a routing protocol with security features enshrined into it to not provide routing efficiency among nodes.

A routing protocol which utilises trust model to determines packet drop in order to identify black hole attack.

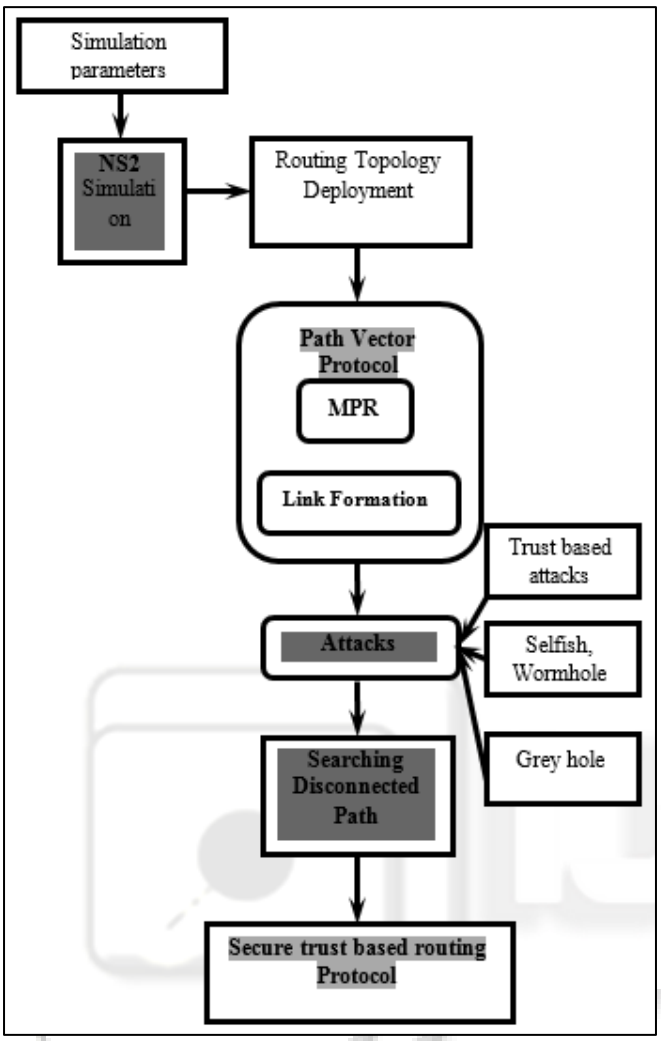
B. Proposed System:

Mobile Ad-hoc networking is a concept in computer communications, which means that users want to communicate with each other form a temporary network, without any form of centralized administration. Each node participating in the network acts both as host and a router and must therefore be willing to forward packets for other nodes. For this purpose, a routing protocol is needed. Novel mechanisms for the Secure routing protocol, aiming to improve its energy performance in Mobile ah-hoc Networks. Routing protocols over MANET are an important issue and many proposals have been addressed to efficiently manage topology information, to offer network scalability and to prolong network lifetime. The proposed system presents a modification in the secure routing protocol with MPR selection mechanism based on the Willingness concept, in order to prolong the network lifetime without losses of performance (in terms of throughput, end-to-end delay or overhead).

1) Advantages:

- The proposed system proves that the exclusion of the energy consumption due to the overhearing can extend the lifetime of the nodes without compromising the routing functioning at all.
- A comparison of trust based approach compromise and packet delivery ratio is better in distributed map detection protocol compared to traditional routing protocols, such as AODV and FSR.

III. ARCHITECTURE DIAGRAM:



IV. FRONT END NETWORK SIMULATOR (NS)

Network simulator 2 is used as the simulation tool in this project. NS was chosen as the simulator partly because of the range of features it provides and partly because it has an open source code that can be modified and extended. Network simulator (NS) is an object–oriented, discrete event simulator for networking research. There are different versions of NS and the latest version is ns-2.1b9a, while ns-2.1b10 is under development, NS provides substantial support for simulation of TCP, routing and multicast protocols over wired and wireless networks. This simulator is a result of an ongoing effort of research and development. Even though there is a considerable confidence in NS, it is not a polished product yet and bugs are being discovered and corrected continuously.

NS is written in C++, with an OTcl1 interpreter as a command and configuration interface. The C++ part, which is fast to run but slower to change, is used for detailed protocol implementation. The OTcl part, on the other hand, which runs much slower but can be changed very fast quickly, is used for simulation configuration. One of the advantages of this split-language program approach is that it allows for fast generation of large scenarios. To simply use the simulator, it is sufficient to know OTcl. On the other hand, one disadvantage is that modifying and extending the simulator requires programming and debugging in both languages.

NS can simulate the following:

1) Topology: Wired, wireless
2) Scheduling Algorithms: RED, Drop Tail,
3) Transport Protocols: TCP, UDP
4) Routing: Static and dynamic routing
5) Application: FTP, HTTP, Telnet, Traffic generators

A. User's View of Ns-2

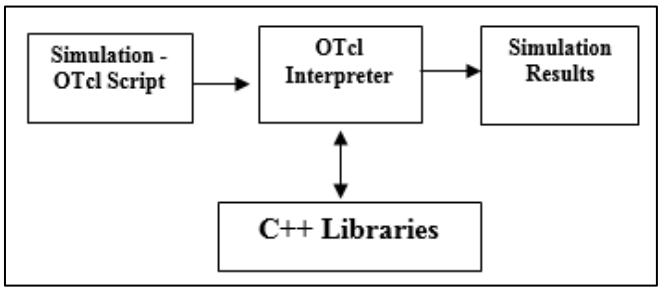


Fig. 4.1: Block diagram of Architecture of NS-2

B. Network Components

This section talks about the NS components, mostly compound network components. Figure 4.1 shows a partial OTcl class hierarchy of NS, which will help understanding the basic network components. The root of the hierarchy is the TclObject class that is the super class of all OTcl library objects (scheduler, network components, timers and the other objects including NAM related ones).

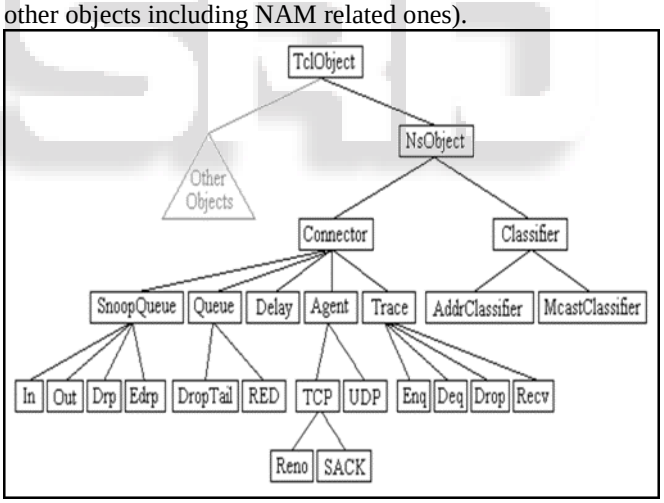
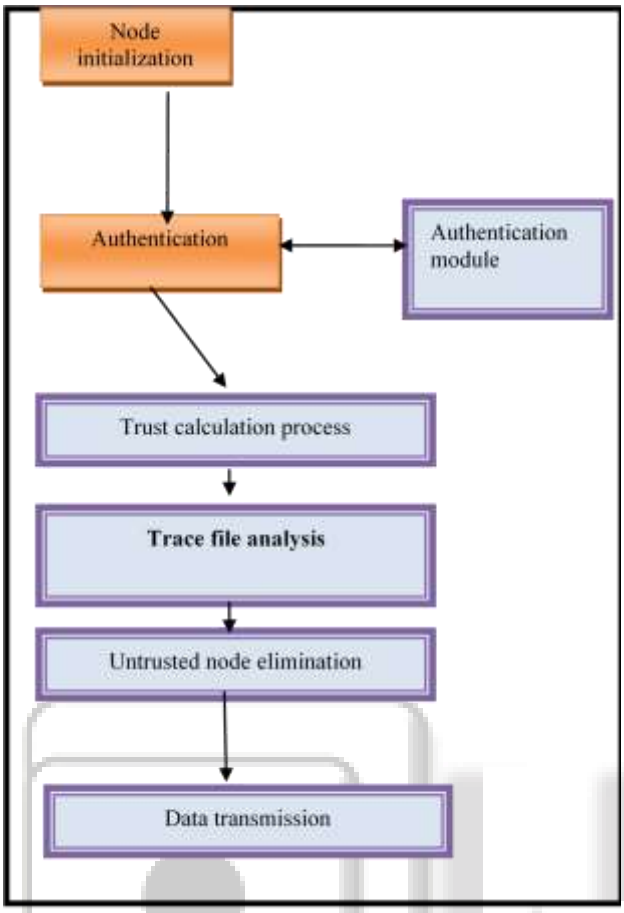


Fig. 4.2 OTcl Class Hierarchies

As an ancestor class of TclObject, NsObject class is the super class of all basic network component objects that handle packets, which may compose compound network objects such as nodes and links was shown in Figure 4.2. The basic network components are further divided into two subclasses, Connector and Classifier, based on the number of the possible output DATA paths. The basic network and objects that have only one output DATA path are under the Connector class, and switching objects that have possible multiple output DATA paths are under the Classifier class.

V. SYSTEM DESIGN

A. System Flow Diagram



VI. MODULE DESCRIPTION

A. Network Model

The network model in this section concerning the Distributed Path Vector (DPV) protocol is taken from its AODV routing. It is a proactive routing protocol, so the routes are always immediately available when needed. DPV is an optimization version of a pure link state protocol. So the topological changes cause the flooding of the topological information to all available hosts in the network. To reduce the possible overhead in the network protocol uses Multipoint Relays (MPR). The idea of MPRis to reduce flooding of broadcasts by reducing the same broadcast public encryption keys in some regions in the network, more details about MPR can be found later in this chapter. Another reduce is to provide the shortest path. The reducing the time interval for the control messages transmission can bring more reactivity DPV uses two kinds of the control messages should be encrypted.

The Hello messages are sent only one hop away but the TC messages are broadcasted throughout the entire network.TC messages are used for broadcasting information about own advertised neighbors which includes at least the MPR Selector list. The TC messages are broadcasted periodically and only the MPR hosts can forward the TC messages.

1) MOBILITY MODELING

The random waypoint model (RWP) is one of the most widely used mobility models in performance analysis of ad hoc networks. The research work analyze the stationary spatial distribution of a node moving according to the RWP model in a given convex area. For this it give an explicit expression, which is in the form of a one-dimensional integral giving the density up to a normalization constant. This result is also generalized to the case where the waypoints have a non-uniform distribution. Additionally, to study a modified RWP model, where the waypoints are on the path boundary. The analytical results are illustrated through numerical examples. Moreover, the analytical results are applied to study certain performance measures in ad hoc networks, namely connectivity and traffic load distribution.

In the network simulator (ns-2) distribution, the implementation of this mobility model is as follows: as the simulation starts, each mobile node randomly selects one location in the simulation field as the destination. It then travels towards this destination with constant velocity chosen uniformly and randomly from [0,V], where the parameter V is the maximum allowable velocity for every mobile node. The velocity and direction of a node are chosen independently of other nodes. Upon reaching the destination, the node stops for a duration defined by the 'pause time' parameter. If T=0, this leads to continuous mobility. After this duration, it again chooses another random destination in the simulation field and moves towards it. The whole process is repeated again and again until the simulation ends.

In the Random Waypoint model, V_{max} and T_{pause} are the two key parameters that determine the mobility behavior of nodes. If the V_{max} is small and the pause time T_{pause} is long, the topology of Ad Hoc network becomes relatively stable. On the other hand, if the node moves fast (i.e.,V_{max} is large) and the pause time T_{pause} is small, the topology is expected to be highly dynamic. Varying these two parameters, especially the V_{max} parameter, the Random Waypoint model can generate various mobility scenarios with different levels of nodal speed.

The proposed the Mobility metric to capture and quantify this nodal speed notion. The measure of relative speed between node i and j at time t is,

$$RS(i,j,t) = \left|V_i(t) - \frac{V_j(t)}{M}\right| \quad (1)$$

Then, the Mobility metric is calculated as the measure of relative speed averaged over all node pairs and over all time. The formal definition is as follows,

$$M = \frac{1}{|i,j|}\sum_{i=1}^{N}\sum_{j=i+1}^{N}\frac{1}{T}\int_0^T RS(i,j,t)dt \quad (2)$$

where |i,j| is the number of distinct node pair (i,j), n is the total number of nodes in the simulation field (i.e., ad hoc network), and T is the simulation time.

Using this Mobility modelis able to roughly measure the level of nodal speed and differentiate the different mobility scenarios based on the level of mobility. The Relative Speed (RS) linearly and monotonically increases with the maximum allowable velocity.

2) Secure Routing Implementation

The secure routing of DPV uses two kinds of the control messages: Hello and Topology Control (TC). Hello messages are used for finding the information about the link status and the host's neighbors. With the Hello message the Multipoint Relay (MPR) Selector set is constructed which describes which neighbors has chosen this host to act as MPR and from this information the host can calculate its own set of the MPRs. the Hello messages are sent only one hop away but the TC messages are broadcasted throughout the entire network. TC messages are used for broadcasting information about own advertised neighbors which includes at least the MPR Selector list. The TC messages are broadcasted periodically and only the MPR hosts can forward the TC messages.

The path in the mobile ad hoc network can be either unidirectional or bidirectional so the host must know this information about the neighbors. The control messages are broadcasted periodically for the neighbor sensing. The control messages are only broadcasted one hop away so that they are not forwarded further. When the first host receives the Hello message from the second host, it sets the second host status to asymmetric in the routing table. When the first host sends a control message and includes that, it has the link to the second host as asymmetric, the second host set first host status to symmetric in own routing table. Finally, when second host send again control message, where the status of the link for the first host is indicated as symmetric, then first host changes the status from asymmetric to symmetric. In the end both hosts knows that their neighbor is alive and the corresponding link is bidirectional.

The Control Messages (CM) are used for getting the information about local links and neighbors. The control messages periodic broadcasting is used for link sensing, neighbor's detection and MPR selection process. Control message contains: information how often the host sends control messages, willingness of host to act as a Multipoint Relay, and information about its neighbor. Information about the neighbors contains:

3) Secure Trust Based Routing Detection Algorithm

The Secure trust based routing detection algorithm predicts the distributed attacks (wormhole, grey-hole, black-hole) in mobile adhoc network. In the detection scheme, every node in the network monitors the behavior of its neighbors and upon detecting any abnormal action by any of its neighbors invokes a distributed algorithm to ascertain whether the node behaving abnormally is indeed malicious. The protocol works through cooperation of some security components that are present in each node in the networks. These components are as follows: (i) discovery, (ii) trust collector, (iii) trust manager, (iv) trust propagator. The functions of these components are described below.

The discovery module of each node passively listens to the communication to and from each of its neighbors. For detecting packet drops and modifications by the neighboring nodes, the monitor module of a node randomly copies the incoming packets to its neighbors and checks whether the neighbors really forward the packets with contents unchanged, or drop them, or modify the contents before forwarding them. The Trust collector module of a node invokes a majority consensus algorithm among the neighbors of a node that has been suspected to be malicious. On being activated by its discovery module, the (accuser) node that has suspected some malicious activity by one of its neighbors challenges the suspicious node to verify its behavior as observed by all of its neighbors. The accused (suspected) node on receiving the challenge responds by acknowledging the message and sending a verify behavior message to all of its neighbors. The neighbors respond by sending the observed value of the degree of maliciousness of the accused node. The accused node calculates the group's trust in its behavior using the received values and broadcasts the computed group-trust along with the received responses to all the neighbors. The messages are also time-stamped so as to prevent replay attacks. For computing group trust value from the received responses, any consensus-based scheme can be used. In the proposed scheme, the difference of the absolute trust values and the average degree of maliciousness of the majority of the respondents (neighbors) has been taken as the final group-trust value of the node. Majority among the neighbors has been taken as the larger of the two subsets of nodes obtained by partitioning the nodes on the basis of a preset threshold value of trust.

Trust Manager: Each node in the network maintains a global trust state containing the suspected nodes and their trust values. A routing table is also maintained that contains a list of nodes that has been determined to be malicious and thus should not be allowed any access to the network resources. The trust manager of a node is responsible for verifying the correctness of the group trust certificate received, caching them, and updating the global trust state (table) of the node for which it has received a new group certificate (from the neighbors of a suspected node).

VII. CONCLUSION AND FUTURE ENHANCEMENT

The research presents a new approach which combines techniques from various fields and adapts to solve the problem of secure routing, shortest path selection and packet detection accuracy. The results show that the proposals generated the extremely relevant. It has been observed that as the packet delivery ratio and Throughput prevents the quality of proposed system. The goal of this research is designed, implemented and evaluated a multi-hop ad hoc network using Secure routing detection Algorithm(SRD)and NS 2.35 Framework. Each secure routing path communicates wirelessly with another using the IEEE 802.11b technology without any aid of infrastructure. The main protocol implemented in this application was the Secure trust based (STB) protocol, which consists of two important mechanisms, Multipoint Relay (MPR) and Shortest path routing. Since the STB protocol operates exclusively based on source routing and on-demand process, it has been selected as the routing protocol to be implemented and tested for our ad hoc messenger application characterized by a source on-demand chat conversation between nodes in a mobile ad hoc network. Some of future woks can include:

The future work can test performance of other routing protocols, such as AODV, DSDV, DSR, geographical forwarding, etc. To compare against the STBprotocol.

In order to optimize the use of constrained resources in an ad hoc network, mobility prediction and battery power conservation techniques can be developed and experimented to test the effect of these ad hoc routing protocols on a real application, such as the real ad hoc messenger developed in the thesis.

REFERENCES

[1] D. Wang and P. Wang, "Understanding Security Failures of Two-Factor Authentication Schemes for Real-Time Applications in Hierarchical Wireless Sensor Networks," Ad Hoc Networks - Elsevier B.V., vol. 20 pp. 1–15, 2016.
[2] L. H. G. Ferraz, P. B. Velloso, and O. C. M. B. Duarte, "An Accurate and Precise Malicious Node Exclusion Mechanism for Ad Hoc Networks," Ad Hoc Networks - Elsevier B.V., vol. 19, pp. 142–155, 2016.
[3] J. Mo, M. Tao, Y. Liu, and R. Wang, "Secure beamforming for mimo two-way communications with an untrusted relay," IEEE Trans. Signal Process., vol. 62, no. 9, pp. 2185–2199, May 2017.
[4] Y. Zou, X. Wang, and W. Shen, "Optimal relay selection for physicallayer security in cooperative wireless networks," IEEE J. Sel. Areas Commun., vol. 31, no. 10, pp. 2099–2111, Oct. 2018.
[5] A. Sheikholeslami, M. Ghaderi, H. Pishro-Nik, and D. Goeckel, "Jamming-aware minimum energy routing in wireless networks," in Proc. IEEE Int. Conf. Commun. (ICC), June 2018, pp. 2313–2318.
[6] Z. Ding, K. Leung, D. Goeckel, and D. Towsley, "On the application of cooperative transmission to secrecy communications," IEEE J. Sel. Areas Commun., vol. 30, no. 2, pp. 359–368, Feb. 2016.
[7] M. Saad, "Joint optimal routing and power allocation for spectral efficiency in multi-hop wireless networks," IEEE Trans. Wireless Commun., vol. 13, no. 5, pp. 2530–2539, May 2014.
[8] C. Wang, H.-M.Wang, and X.-G. Xia, "Hybrid opportunistic relaying and jamming with power allocation for secure cooperative networks," IEEE Trans. Wireless Commun., vol. 14, no. 2, pp. 589–605, Feb 2015.
[9] J. Li, A. Petropulu, and S. Weber, "On cooperative relaying schemes for wireless physical layer security," IEEE Trans. Signal Process. vol. 59, no. 10, pp. 4985–4997, Oct. 2011.
[10] C. Ma, J. Liu, X. Tian, H. Yu, Y. Cui, and X. Wang, "Interference exploitation in d2d-enabled cellular networks: A secrecy perspective," IEEE Trans. Commun., vol. 63, no. 1, pp. 229–242, Jan. 2015

