Volume 4, Issue 8, August 2014 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

An Efficient Malicious Nodes Detection in MANETs using OPNET

Gajendra Singh Baghel
Information Technology Department
SSSIST, RGPV
Sehore, M.P., India

Vandana Chourewar
Information Technology Department
SSSIST, RGPV
Sehore, M.P., India

Abstract— Ad-hoc Networks (MANETs) square measure extraordinarily susceptible to a range of misbehaviors due to their basic advantages, together with lack of communication infrastructure, short transmission power, and dynamic network configuration. To observe and mitigate those misbehaviors, several trust management schemes are given for MANETs. Most suppose pre-defined weights to work out however every apparent misconduct contributes to associate overall calculate of belief. The extraordinarily dynamic nature of MANETs makes it tough, however, to work out a collection of weights that area unit applicable for all contexts. We have described an automatic trust management method for MANETs that uses machine learning to classify nodes as malicious. Our theme is much a lot of resilient to the context changes common in MANETs, like those because of malicious nodes sterilization their wrongful conduct patterns over time or speedy changes in environmental factors, like the motion speed and transmission vary. This work compares our method to existing approaches and current analysis results obtained from simulation studies. This paper introduced new planned algorithmic rule for management system in Ad-hoc networks within opnet simulator environment

Keywords— misbehaviours, malicious, opnet, MANETs, Detection.

I. INTRODUCTION

Ad hoc networks are a new model of wireless information exchange for mobile device known as node. In an ad hoc network, there is no permanent setup such as base stations or movable exchange hub. Mobile nodes that are inside each other's transmission range sends information data straight using wireless links, whereas those that are far away from other nodes to pass on data packet as routers. Node mobility in an ad hoc system reasons regular changes of the network topology. Figure 1 shows such an instance, as shown situation at first, nodes A and D have a straight connection link connecting them. When D moves out of A's transmission range, the connection link is broken. Still, the network is remain linked, because A be able to contact D throughout C, E, as well as F. Military intentional procedures are still the main application of ad hoc networks now. For example, military elements (e.g., soldiers, tanks, or planes), prepared with wireless communication devices, could figure out an ad hoc network while they roam in a combat zone. Ad hoc networks also able to use for urgent situations like law enforcement, and rescue missions, disasters. While MANET can be installs quickly with pretty little cost, it grows to be a striking choice for business uses such as sensor networks or virtual classrooms.

Security is an essential matter for ad hoc networks, mainly for individual's security-sensitive purposes. To protect an ad hoc network, we suppose the subsequent characteristics: accessibility, privacy, integrity, verification, and non-repudiation.

Accessibility: Accessibility ensures the survivability of network services even though denial of service attacks. A denial of service attack might be initiate at whichever layer of an ad hoc network. Going on the physical as well as media access control level, an antagonist might utilize blocking to interfere by communication on physical control. Taking place the network layer, an antagonist can interrupt the routing protocol and cut off the network. On top of the upper layers, a challenger might bring along high-level services. Individual such objective is the primarily management service, a necessary service for every security framework.

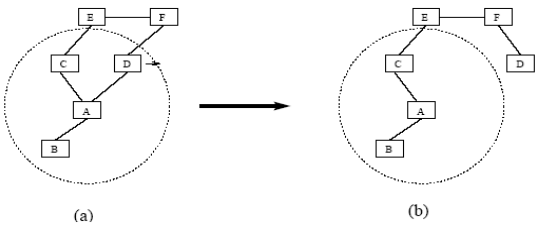

Fig 1. Topology change in ad hoc networks: nodes A, B, C, D, E, and F constitute an ad hoc network. The circle represents the radio range of node A. The network initially has the topology in (a). When node D moves out of the radio range of A, the network topology changes to the one in (b).

Privacy: Privacy guarantees that given information is not at all reveal to unauthorized individuals. Network communication of sensitive information, for example intentional or deliberate forces information, involves privacy. Outflow of such information to opponent can have shocking consequences. Routing information necessity as well residue secreted in positive cases, since the information may be important for opponents to recognize and to set their targets in a combat zone.

Integrity: Integrity assurance to facilitate a message being transmitted is not at all despoiled. A message can be despoiled since of caring malfunction, for instance radio broadcast harm, or for the reason that of malicious attacks on the network.

Verification: Verification allows a node to make sure the validity of the examiner node it is communicating with. Without verification, an antagonist can pretend to be a node, therefore gaining not permitted rights to resource and susceptible information and intrusive with the action of further nodes.

At last, non-repudiation ensures that the foundation of a message cannot deny comprise sent the message. No repudiation is helpful for discovery and separation of concession nodes. While a node A gets an incorrect message from a node B, non-repudiation permits A to indict B via this message and to induce other nodes that B is compromised.

Intrusion Detection is an action with the intention of resolve whether a procedure or client is efforts for somewhat unpredicted. It's working as distinct by Michael G Solomon and Mike Chappel [1] on the foundation of investigative action on a particular device or network with decide whether the action is common or mistrustful. It can moreover compare recent action to recognized attack prototype or just raise an alarm circumstance while detailed measurements go over specific standards.

There have been a lot of techniques for intrusion recognition in MANETs. The preliminary categorizations are found on validation based systems. These rely on the recognition of nodes through an only identifier. Make use of encryption keys comes into this category, as well as they have been sincerely deliberate. The subsequent approach is behavioral base algorithms by this intrusion can be distinct based on nodal behaviors, rather than its identifier. This, according to us, is an enhanced approach for the given reasons:

1. Node uniqueness can be simply tolen, Behavior is tougher to replicate.
2. individuality based actions involves storage of Identifier databases or judgment.
3. Every fresh node has to be specified a unique identifier, construction the procedure of deployment additional expensive (time and cost).

Thus, we bound our focal point to intrusion detection supports on activities, as we believe it is an extra competent, lightweight and effortlessly scalable explanation to Intrusion Detection in MANETs. The segments that pursue such systems. Intrusion Detection Systems based on performance is able to be generally classified into following categories: anomaly detection, signature or misuse detection moreover specification based detection. We state these as per the categorization proposed in [2].

II. RELATED WORK

In the past decade, many research efforts have been made to address the security needs for MANETs by means of trust management Cho, Swami [6]. The main goal of trust management is to evaluate the actions of other nodes, and build a reputation for each node based on the node evaluation result. The reputation can then be used to determine the trustworthiness for other nodes. The trustworthiness can be utilized to make choices on which nodes to cooperate with, or even take action to punish an untrustworthy node if necessary. Trust is divided into direct trust and indirect trust Theodorakopoulos and Baras [7]. Direct trust stems from the first-hand observations locally obtained by a node itself, while indirect trust refers to the secondhand observations released by other nodes. In MANETs, direct trust cannot always provide comprehensive evaluation of the target node due to exterior circumstances such as channel conditions, temporary unavailability, interference, etc. At this time, indirect trust is used to provide secondary information to help evaluate the actual trustworthiness of the target node.

In [3], Buchegger et al. proposed the CONFIDANT protocol to encourage the node cooperation and punish misbehaving nodes. Michiardi et al. [4] presented a mechanism with the name CORE to identify selfish nodes, and then compel them to cooperate in the following routing activities. Patwardhan et al. [9] studied an approach in which the reputation of a node is determined by data validation. In our previous research work Li and Finin [5], Li, Parker [8], we proposed a multi-dimensional trust management scheme for MANETs. In this framework, the trustworthiness of a node is judged from different perspectives (i.e., dimensions), and each imension of the trustworthiness is derived from various sets of misbehaviors according to the nature of those misbehaviors.

When it comes to the discussion of misbehavior detection, we should first clearly understand the term misbehavior itself. Note that the term misbehavior generally refers to abnormal behavior that deviates from the set of behaviors that each node is supposed to conduct in MANETs Buchegger and Lee [14]. According to Yau and Mitchell [15], there are four types of misbehaviors in ad hoc networks, namely failed node behaviors, badly failed node behaviors, selfish attacks, and malicious attacks. These four types of node misbehaviors are classified with respect to the node's intent and action. More specifically, selfish attacks are intentional passive misbehaviors, where nodes choose not to fully participate in the packet forwarding functionality to conserve their resources, such as battery power; malicious attacks are intentional active misbehaviors, where the malicious node aims to purposely interrupt network operations. The existence of selfishness and malicious behaviors has remarkably motivated research in the area of misbehavior detection for mobile ad hoc networks. Intrusion Detection System (IDS) is normally regarded as an important solution for detecting various

node misbehaviors in MANETs. Several approaches have been proposed to build IDS probes on each individual peer due to the lack of a fixed infrastructure, such as Zhang and Lee [10], Deng, Zeng [16], Tseng, Balasubramanyam [17]. In these approaches, there is one IDS probe installed on each node, and each IDS probe is assumed to be always monitoring the network traffic, which is obviously not energy efficient given the limited battery power that each node has in MANETs. In contrast, Huang et al. [13] proposed a cooperative intrusion detection framework in which clusters are formed and the nodes in each cluster will fulfill the intrusion detection task in turn.

This cluster-based approach can noticeably reduce the power consumption for each node. Routing misbehaviors are another major security threats that have been extensively studied in ad hoc networks. In addition to externally intruding into MANETs, an adversary may also choose to compromise some nodes in ad hoc networks, and make use of them to disturb the routing services so as to make part of or the entire network unreachable. Marti et al. [11] introduced two related techniques, namely watchdog and pathrater, to detect and isolate misbehaving nodes, which are nodes that do not forward packets. There are also some other solutions that aim to cope with various routing misbehaviors Anderegg and Eidenbenz [18], Kefayati, Rabiee [20].

We have also made some efforts to address the problem of misbehavior detection in ad hoc networks [21], [22], [23]. In our initial work Li, J. Parker [21], we have done a preliminary study where outlier detection method is adopted to identify node misbehaviors. The work in Li and A. Joshi [22] extends the idea in that both weighted voting and the Dempster-Shafer Theory of evidence (DST) are used to combine multiple pieces of evidences from different observations in order to detect the node misbehaviors in a more accurate manner. In our latest work Joshi, and T. Finin [23], policy as well as context information have been utilized to reveal the difference between the truly malicious nodes and the faulty ones, both of which may be treated as misbehaving nodes with no difference in most of existing misbehavior detection mechanisms.

However, each dimension of trustworthiness is still derived from a predefined formula with a set of fixed weights, which still cannot well adapt to complicated scenarios or context changes.

III. MISBEHAVIOR DETECTION

As we have discussed in the previous section, the gossip based outlier detection algorithm is used in the Misbehavior Detector to identify misbehaving nodes. The outlier detection algorithm has the following four steps, viz. local view formation, local view exchange, view combination, and global view formation. The basic functionality of the Misbehavior Detector is similar to the outlier detection algorithm that we have proposed earlier [24]. However, the context information offered by the Policy Manager is added to the outlier detection algorithm, and the context information is used to decide the circumstance under which the misbehaviors occur. In this way, a node may distinguish a malicious node from other faulty nodes because they carry out the misbehaviors under different circumstances.

IV. PROPOSED WORK

The term node is defined as a system entity in MANETs that owns a tiny processor that has limited computational capability as well as a wireless Network Interface Card (NIC) with a bounded radio transmission range. Moreover, we also assume that each node is capable of observing the behaviors of other nodes within its radio transmission range, and exchanging these observations with other nodes in its radio transmission range. Denote a neighbor of a node A as a node that resides within A's radio transmission range. The type of abnormal behaviors that each node observes can be defined by the nodes themselves as long as all the nodes observe the same set of abnormal behaviors. While a node observes the abnormal behaviors that its neighbors conduct, it also keeps track of the total amount of incoming packets it has observed for each neighbor. When a node needs to summarize its observation and thereby form its local view of misbehaving nodes, it will calculate the rate of abnormal behaviors over the overall behaviors it has observed for the node.

While a node observes the abnormal behaviors that its neighbors conduct, it also keeps track of the total amount of incoming packets it has observed for each neighbor. When a node needs to summarize its observation and thereby form its local view of misbehaving nodes, it will calculate the rate of abnormal behaviors over the overall behaviors it has observed for the node. For instance, if all the nodes choose to observe the behaviors of packet drop, modification and misroute, then packet drop rate (PDR), packet modification rate (PMOR) and packet misroute rate (PMIR), average packet delay (Delay) can be defined as follows, respectively.

PDR = Number of Packet Dropped/Total Number of Incoming Packets

PMOR = Number of Packet Modified/Total Number of Incoming Packets

PMIR = Number of Packet Misrouted/Total Number of Incoming Packets

Delay = Sum of Time taken to deliver all packets/(Total Number of Incoming Nodes.

A. PROPOSED Method

The security management framework has two functional modules: Behavior Data Collection and Trust Management.

1 Behavioral Data Collection

The behavioral data collection module is responsible for the collection of node behaviors and formation of behavioral dataset. In this paper, a node's behavior is described in terms of the ratio of the amount of this behavior over the total amount of packets that the node has received, such as packet drop ratio (PDR), packet modification ratio (PMOR), packet miss ratio (PMIR) and packet delay.

We use network simulations to generate behavioral dataset and classifier as malicious or normal node. Because the adversaries and their misbehaviors are pre-defined in these simulations, the behavioral data are collected and then labeled

according to the ground truth regarding adversaries. An example training dataset is shown in Table I. Here, we create a m-dimensional feature vector for each node. In the example shown in Table I, m = 4. During the testing stage, the Behavioral Data Collection module on each node first observes and records the behaviors of their neighbors. It also receives and integrates node behaviors reported by other nodes.

Table 1 Training dataset

Node ID	PDR	PMOR	PMIR	Delay
1	90%	10%	0	50ms
2	2%	0	0	15ms
3	30%	60%	10%	80ms
4	5%	0	0	10ms
5	10%	0	90%	60ms
• • •	• • •	• • •	• • •	• • •

B. Malicious Node Detection Algorithm

For this we will use following metrics for behavior classification-

(1) PDR(Packet Data Rate)-

PDR= (Number of Packet's Dropped)/ (Total Number of Incoming Nodes)

(2) PMOR (Packet Modification Rate)-

PMOR= (Number of Packet's Modified)/ (Total Number of Incoming Nodes)

(3) PMIR(Packet Misroute Rate)-

PMIR= (Number of Packet's Misrouted)/ (Total Number of Incoming Nodes)

(4) Delay (Average Packet Delay)-

Delay = Sum of Time taken to deliver all packets/ (Total Number of Incoming Nodes)

Mobility Model's used for MANET topology-

(1) Constant Acceleration Mobility Model.

(2) Constant Position Mobility Model.

(3) Constant Velocity Mobility Model.

(4) Random Way-point Mobility Model.

Systematic algorithm can be given as following steps.

C. Proposed Algorithm

OPNET Simulation

1. Design Wi-Fi topology using MANET
2. Select MAC, IP and Application protocol on each node.
3. Select MANET routing protocol AODV start simulation
4. For each node i
   a. do
   b. RREQ start (in case of AODV)
   c. Flooding of RREQ
   d. Build routing table
      i) Collect behaviors statistics such as No. of packet transmitted, received, lost, delay time, modified etc.
      ii) Store data in xml format using opnet statics utility

Behavior Classification

1. Input .xml/.csv data file Generated by OPNET
2. Calculate PDR, PMOR and PMIR using DOM for each node in network.
   a. For each node i repeat
   b. Compare PDR, PMOR and PMIR for Threshold value.
3. Result displayed using java as Malicious node and authenticate node.

V. SIMULATION RESULTS

As proposed algorithm have two phase one is malicious node detection hence simulation also have done in two part in first part OPNET is used to create MANET with AODV routing protocol for path finding and generate row packet transmission to capture node behavior as their packet drop, packet misroute and packet modified data collection for every node in Network. This data collection is done by running simulation for 20 minutes with different numbers of node as 40, 60, 80, 100, 120, 140, 160 with all default configurations. After getting packet statics these data saved in xml format by using OPNET export data utility.

Our simulator is written in the JAVA language. We assume there is no loss at the communication level for proposed algorithm. In a typical simulation, our program generates a random network topology according to some input parameters. Then the CH selection algorithms are executed by the nodes on this network topology and the parameters of interest are reported. The input parameters are the total number of nodes n in the network, the average node density.

A. Simulation Parameter

Following table 2 gives all parameter used for simulation. we have used under our JAVA simulator.

Table 2 Simulation Parameter Details.

Parameter	**Value**
Network Size	400*400
Mobility Model	Random Waypoint model
Nodes (WifiNode's)	40, 60, 80, 100, 120, 140, 160 nodes
Update Interval	100s
Node Speed	10 m/s
Traffic Model	Constant Bit Rate
Transmission Range	50, 70
Threshold Value of PDR	8%
Threshold Value of PDR	8%
Threshold Value of PDR	8%

B. Simulation Snapshot

In this work OPNET simulator is used to detect a node behavior as malicious or normal node if any node is abnormal it will terminate from cluster for more reliable cluster formation. OPNET stood for Optimized Network Engineering Tools. OPNET is a Modeler, a software tool for network modeling and simulation. Figure 1 show snapshot of simulation during result capturing in OPNET. OPNET simulation for desire network size here an example of network size 40 node and network area is 1000*1000 meter.

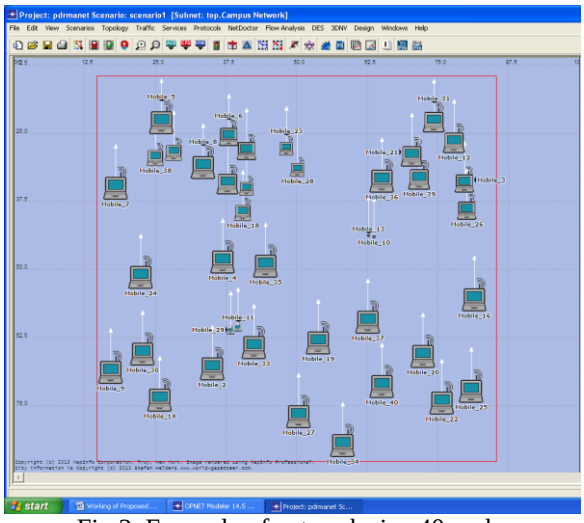

Fig 2. Example of network size 40 node

VI. RESULT AND DISCUSSION

Above figure 3 and 4 shows a snapshot during simulation of proposed algorithm at this instance number of nodes in figure 2 are 20 where having number of nodes are 40 with same transmission range in both figure is 50 units we have consider unit is meter here.

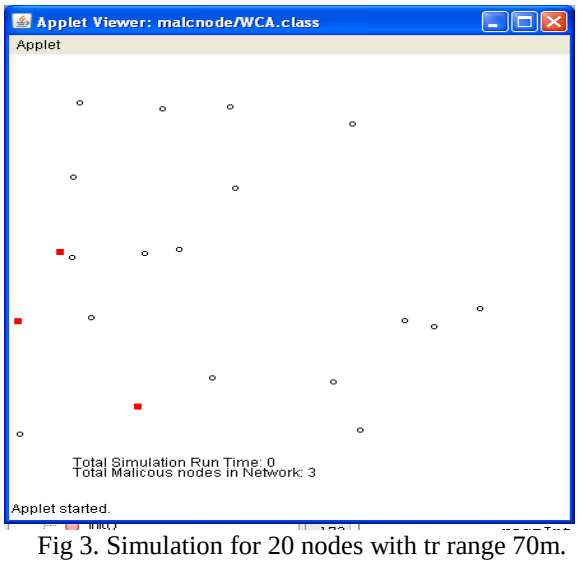

Fig 3. Simulation for 20 nodes with tr range 70m.

For node packet statics behaviour analysis figure 4 give all detail of node packet transmission behaviour as packet drop ratio PDR, packet missroute ration PMR and packet modified ration shown in legends as PMOR this figure is statics when network having 40 nodes and OPNET simulation runs for 20 minites.

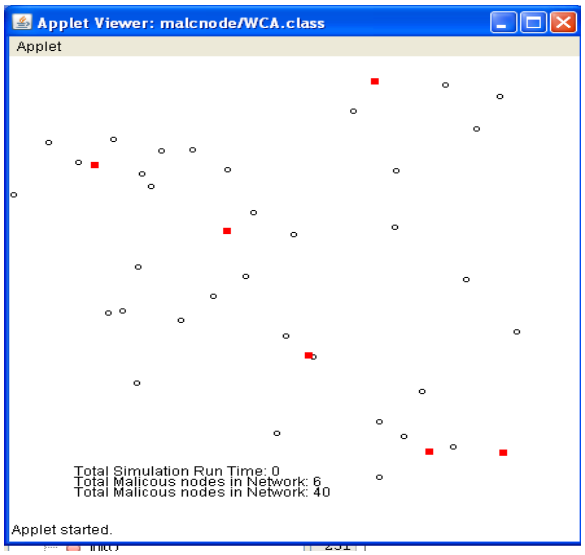

Fig 4. Simulation for 40 nodes with tr range 70m.

This Figure 5 shows malicious nodes detected during simulation run on OPNET for different nodes as 40, 60, 80, 100, 120, 140 and 160 for 20 minutes.

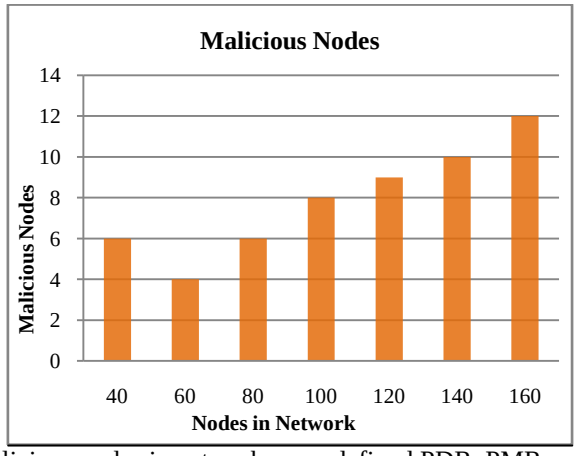

Fig 5. Detection of malicious nodes in network as predefined PDR, PMR and PMOR threshold value.

VII. CONCLUSION

Selfish nodes refuse to take exposed networking responsibilities for others although silent applying and using the facilities offered through others within the network. They disregard all data and control packets so as to be not intended to them, preserve resources in favor of their self to the highest. The unstable resource utilization of IDs in MANET and occurrence of selfish nodes are the two essential problems in movable Ad-hoc Network. It is resolved through with malicious node discovery. Within this effort, we have examined the safety threats an ad hoc network appearance and offered the security objectives to facilitate necessitate to be accomplish. On one offer, the security-sensitive claims of ad hoc networks involve high amount of security; on the other offer, ad hoc networks are inherently susceptible to safety attacks. Consequently, security apparatus are crucial for ad hoc networks. The habit of ad hoc networks causes both challenge and chance for these methods.

We aimed to determine a method to identify malicious or compromised nodes in a MANET with mobile nodes based on behavioral attributes and formed cluster on basis of node weight combining their key parameters such as neighbor, node movement speed, and direction of movement and battery power of node for efficient and stable cluster.

It is solved by using improved weighted clustering algorithm for cluster formation and cluster head election mechanism. This model is able to prolong the life time of MANET, decrease the percentage of leader nodes, maximize the cluster size decreases the computation delay, maintain stability of cluster and keep security from selfish nodes.

REFERENCES

[1] Michael G Solomon and Mike Chappel. Information Security Illuminated. Jones and Bartlett, 2004.

[2] Amitabh Mishra, Ketan Nadkarni, and Animesh Patcha. Intrusion detection in wireless ad hoc networks. IEEE wireless communications, February 2004.

[3] S. Buchegger and J.-Y. Le Boudec, "Performance analysis of the confidant protocol," in MobiHoc '02: Proceedings of the 3rd ACM international symposium on Mobile ad hoc networking & computing. New York, NY, USA: ACM, 2002, pp. 226–236.

[4] P. Michiardi and R. Molva, "Core: a collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks," in Proceedings of the IFIP TC6/TC11 Sixth Joint Working Conference on Communications and Multimedia Security. Deventer, The Netherlands, The Netherlands: Kluwer, B.V., 2002, pp. 107–121.

[5] W. Li, A. Joshi, and T. Finin, "Coping with node misbehaviors in ad hoc networks: A multi-dimensional trust management approach," in Proceedings of the Eleventeenth International Conference on Mobile Data Management, 2010. MDM '10. IEEE Computer Society, May 2010.

[6] J. Cho, A. Swami, and I. Chen, "A survey on trust management for mobile ad hoc networks," Communications Surveys Tutorials, IEEE, vol. PP, no. 99, pp. 1 –22, 2010.

[7] G. Theodorakopoulos and J. S. Baras, "Trust evaluation in ad-hoc networks," in WiSe '04: Proceedings of the 3rd ACM workshop on Wireless security. New York, NY, USA: ACM, 2004, pp. 1–10.

[8] W. Li, J. Parker, and A. Joshi, "Security through collaboration and trust in manets," ACM/Springer Mobile Networks and Applications (MONET), pp. 1–11, 2010 (Online First).

[9] A. Patwardhan, A. Joshi, T. Finin, and Y. Yesha, "A data intensive reputation management scheme for vehicular ad hoc networks," in Proceedings of the 3rd Annual International Conference on Mobile and Ubiquitous Systems - Workshops, Mobiquitous '06., July 2006, pp. 1–8.

[10] Y. Zhang and W. Lee, "Intrusion detection in wireless ad-hoc networks," in MobiCom '00: Proceedings of the 6th annual international conference on Mobile computing and networking. New York, NY, USA: ACM, 2000, pp. 275–283.

[11] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," in MobiCom '00: Proceedings of the 6th annual international conference on Mobile computing and networking. New York, NY, USA: ACM, 2000, pp. 255–265.

[12] S. Buchegger and J.-Y. Le Boudec, "Performance analysis of the confidant protocol," in MobiHoc '02: Proceedings of the 3rd ACM international symposium on Mobile ad hoc networking & computing. New York, NY, USA: ACM, 2002, pp. 226–236.

[13] Y.-A. Huang and W. Lee, "A cooperative intrusion detection system for ad hoc networks," in SASN '03: Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks. New York, NY, USA: ACM, 2003, pp. 135–147.

[14] S. Buchegger and J.-Y. Le Boudee, "Self-policing mobile ad hoc networks by reputation systems," IEEE Communications Magazine, vol. 43, no. 7, pp. 101–107, July 2005.

[15] P.-W. Yau and C. J. Mitchell, "Security vulnerabilities in ad hoc networks," in Proceedings of the 7th International Symposium on Communication Theory and Applications, 2003, pp. 99–104.

[16] H. Deng, Q.-A. Zeng, and D. Agrawal, "Svm-based intrusion detection system for wireless ad hoc networks," in Proceedings of 2003 IEEE 58th Vehicular Technology Conference, 2003. VTC 2003-Fall., vol. 3, Oct. 2003, pp. 2147–2151.

[17] C.-Y. Tseng, P. Balasubramanyam, C. Ko, R. Limprasittiporn, J. Rowe, and K. Levitt, "A specification-based intrusion detection system for aodv," in SASN '03: Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks. New York, NY, USA: ACM, 2003, pp. 125–134.

[18] L. Anderegg and S. Eidenbenz, "Ad hoc-vcg: a truthful and cost-efficient routing protocol for mobile ad hoc networks with selfish agents," in MobiCom '03: Proceedings of the 9th annual international conference on Mobile computing and networking. New York, NY, USA: ACM, 2003, pp. 245–259.

[19] Y. Xue and K. Nahrstedt, "Providing fault-tolerant ad hoc routing service in adversarial environments," Wirel. Pers. Commun., vol. 29, no. 3-4, pp. 367–388, 2004.

[20] M. Kefayati, H. R. Rabiee, S. G. Miremadi, and A. Khonsari, "Misbehavior resilient multi-path data transmission in mobile ad-hoc networks," in SASN '06: Proceedings of the fourth ACM workshop on Security of ad hoc and sensor networks. New York, NY, USA: ACM, 2006, pp. 91–100.

[21] W. Li, J. Parker, and A. Joshi, "Security through collaboration in manets," in Proceedings of 4th International Conference on Collaborative Computing: Networking, Applications and Worksharing, CollaborateCom 2008, ser. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering (LNICST), vol. 10. Springer, 2008, pp. 696–714.

[22] W. Li and A. Joshi, "Outlier detection in ad hoc networks using dempster-shafer theory," in Proceedings of the Tenth International Conference on Mobile Data Management: Systems, Services and Middleware, 2009. MDM '09., May 2009, pp. 112–121.

[23] W. Li, A. Joshi, and T. Finin, "Policy-based malicious peer detection in ad hoc networks," in Proceedings of the International Conference on Computational Science and Engineering, 2009. CSE '09., vol. 3, Aug. 2009, pp. 76–82.

[24] J. J Garcia-Luana-Aceves and S. Murthy. An Efficient Routing protocol for Wireless Networks. ACM Mobile Networks and Applications Journal, pages 183–197, October 1996.

