International Journal of Electrical and Electronic Engineering & Telecommunications

ISSN 2319 – 2518 www.ijeetc.com
Special Issue, Vol. 1, No. 1, March 2015
National Level Technical Conference P&E- BiDD-2015

Research Paper

AGENT BASED ROUTING FOR WORM HOLE ATTACK IN MANET

Selvin Pradeep Kumar S[1]* and Ajitha L[2]

*Corresponding Author: Selvin Pradeep Kumar S, ✉selvinpradeepkumar@gmail.com

The existence of misbehaving nodes may paralyze the routing operation in MANET. To overcome this behavior that trustworthiness of the network nodes should be consider in the route selection process combined with the next count. The trustworthiness is achieved by measuring the trust value for each node in the network. In this paper a new protocol based on agent based monitoring followed the Dynamic Source Routing (DSR) algorithm is presented. This protocol is applied in agent based trusted Dynamic source routing protocol for MANET's. The objective of this protocol is to mange trust information among self nodes with minimal overhead in terms of time delay and data loss. This objective is achieved through Collaborative Agent Monitoring System (CAMS) by installing in each participated node in the network. CAMS Consist of two types of agent: Self monitoring agent and routing agent. A proposed realistic objective model for measuring trust value is introduced. One of the significant attack in ad hoc network is wormhole attack is more hidden in character and tougher to detect. In this paper an Attitude Agent Intrusion Detection System (AAIDS).

Keywords: Routing, Worm hole, Intrusion, Detection

INTRODUCTION

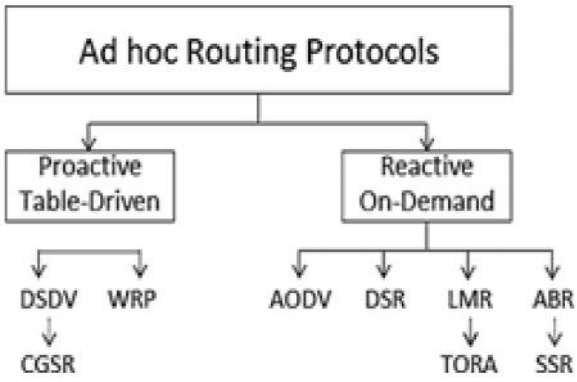
Mobile ad-hoc networks (MANETs) are a collection of mobile nodes which communicate with each other via multi-hope wireless links. Each node in MANETs must act as a router as well as host at the same time. MANETs routing protocols are classified into two categories, table-driven (proactive) and on-demand (reactive) as shown in Figure 1 [1]. On-demand routing protocols which are considered in this paper perform better with significantly lower overheads than table-driven routing protocols in many situations [2].

In general, both types of routing protocols for MANETs are designed based on the assumption that all participating nodes are fully cooperative. Due to MANETs characteristics such as openness, mobility, dynamic topology

[1] ECE Department, Jeppiaar Institute of Technology.

[2] ECE Department, Kings Engineering College.

Figure 1: Categorization of Ad Hoc Routing Protocols



and protocol weaknesses, these may be targeted by attackers in a number of ways [3, 4]. Several "secure" routing protocols have been proposed for MANETs [5-8]. Most of them assume centralized units or trusted third parties, which actually destroy the self-organization nature of MANETs. These protocols are effective to fight against external attacks, but are not able to prevent selfishness like misbehaviors. For example, a node may refuse to forward data packets for other nodes to save its battery. So a comprehensive approach is necessary for MANETs to prevent both attacks and misbehaviors. This approach is regarding the security improvement of the above mentioned protocols. This is achieved by developing mechanisms for measuring the trustworthiness of the net-work nodes. The measure of the trustworthiness of such nodes is through a term called trust level, which results in what is called trusted routing protocols. Many trusted routing protocols have been suggested as an effective security mechanism in MANETs [9-15]. In these protocols, measuring the node's trust level is challenging issue due to the characteristics of MANETs [16].

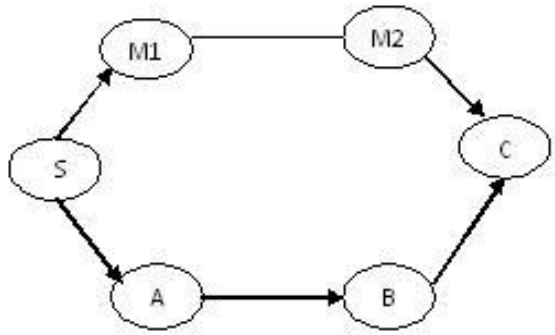
The main presumptions of intrusion detection are these: the client and program activities are noticeable by means of system auditing mechanisms. More significantly, regular and intrusion actions have a distinct behavior. Intrusion detection, therefore, entails capturing audit data and analyzing about the proof in the data to decide whether the system is under attack or not. Depend on the form of audit data adopted, Intrusion Detection System (IDS) can be categorized as host-based or network-based. A network-supported IDS normally operates at the entrance of a network. IDS detain and scrutinize packets that run through the network hardware interface [1]. A host-based IDS relies on operating system audit data to observe and analyze the events created by clients or programs on the host. Intrusion exposure methods can be labeled into anomaly detection and misuse detection [2].

The misuse detection systems exploit models of renowned attacks or frail spots of the system to match and identify known intrusions. The main drawback is that it lacks the capability to detect the truly novel attacks. Anomaly detection subsystems monitor activities that move away significantly from the standard normal usage profiles as anomalies. The main advantage of anomaly detection is that it does not need previous details of invasion and can thus detect new intrusions. The main short-coming is that it may not be able to depict what the attack.

Worm Hole Attack

Wormhole attack is also called the tunneling attack. An attacker receives a packet at one point and tunnels it to another malicious node in the network. This way beginner assumes that he found the shortest path in the network. This

Figure 2: Wormhole Attack



tunnel between two colluding attackers is called the worm hole [1, 2 and 3].

ROUTING, ADDRESSING MISBEHAVIOR PROBLEMS (RAM)

The ultimate goal of the security solutions for MANETs is to provide security services, such as authentication, confidentiality, integrity, anonymity, and availability, to mobile users. In order to achieve this goal, the security solution should provide complete protection spanning the entire protocol stack. In this section we consider a fundamental security problem in MANET: the protection of its basic functionality to deliver data bits from one node to another. In other words, we seek to protect the network connectivity between mobile nodes over potentially multi-hop wireless channels, which is the basis to support any network security services. Multi-hop connectivity is pro-vided in MANETs through two steps: (1) ensuring one-hop connectivity through link-layer protocols (e.g., wireless medium access control, MAC); and (2) extending connectivity to multiple hops through network layer routing and data forwarding protocols (e.g., ad hoc routing). The ultimate multi-fence security solution naturally spans both layers, as illustrated in Figure 2. Due to the absence of a clear line of defense, a complete security solution for MANETs should integrate both approaches and encompass all three components: prevention, detection, and reaction [18].

In the MANET context, the prevention component is mainly achieved by secure ad hoc routing protocols that prevent the attacker from installing incorrect routing states at other nodes. These protocols are typically based on earlier ad hoc routing protocols, and employ different cryptographic primitives (e.g., keyed-Hash Message Authentication Code (HMAC), digital signatures, hash chains) to authenticate the routing messages. The detection component discovers ongoing attacks through identification of abnormal behavior exhibited by malicious nodes. Such misbehavior is detected either in an end-to-end manner, or by the neighboring nodes through overhearing the channel and reaching collaborative consensus. Once an attacker node is detected, the reaction component makes adjustments in routing and forwarding operations, ranging from avoiding the node in route selection to collectively excluding the node from the network.

The routing protocols that have been proposed assume that the nodes will fully participate. Unfortunately, node misbehavior is a common phenomenon. Misbehaving nodes at the routing level can be classified into two main categories:

Selfish Node: operates normally in the Route Discovery and the Route Maintenance phases of the routing protocol. However, it does not perform the packet forwarding function for data packets unrelated to itself. The selfish node

attempts to benefit from other nodes, but refuse to share its own resources.

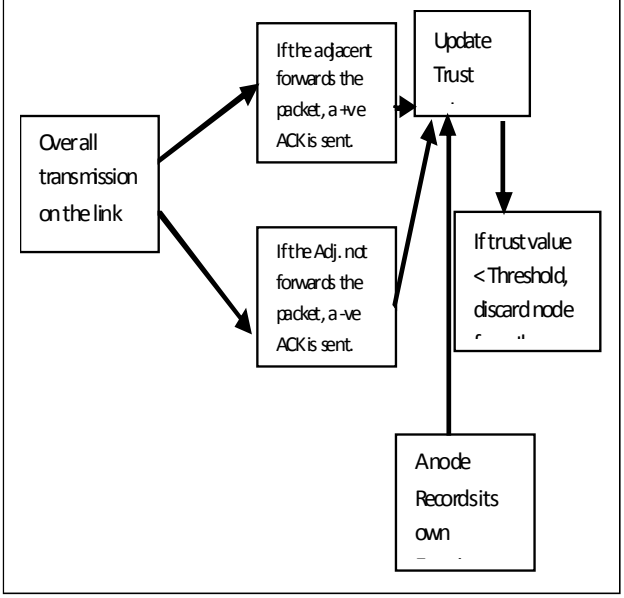
Malicious Node: acts to the detriment of the network by manipulating routing. Many routing protocols use hop count as a metric. A node can falsely claim a low hop count to a destination, enabling it to intercept traffic for that destination. Node identities are not authenticated, so a node can claim to be the destination of a route.

Since such misbehaving nodes participate in the Route Discovery phase, they may be included in the routes chosen to forward the data packets from the source. The misbehaving nodes, however, refuse to forward the data packets from the source. So, the existence of misbehaving nodes may paralyze the routing operation. The adverse effect of routing misbehavior will be illustrated in the context of DSR in Section VI; the simulation results motivates our development of an efficient approach for detecting and mitigating routing misbehavior.

RELATED WORK

In the literature, several researches have been done to enhance the security, misbehavior detection as well as trust management [11, 20-26]. There are common basic functions among the reviewed trust models as summarized in Figure 3, in each model, these functions are executed differently. The nodes watch out their neighbors during a communication and send a report to the members of the network. Each node updates the trust about its neighbors by combining the reports about them and that node's experience with the neighbors. If a node's experience is less than a certain threshold, then it is excluded from the network.

Figure 3: Functions of Trust Models

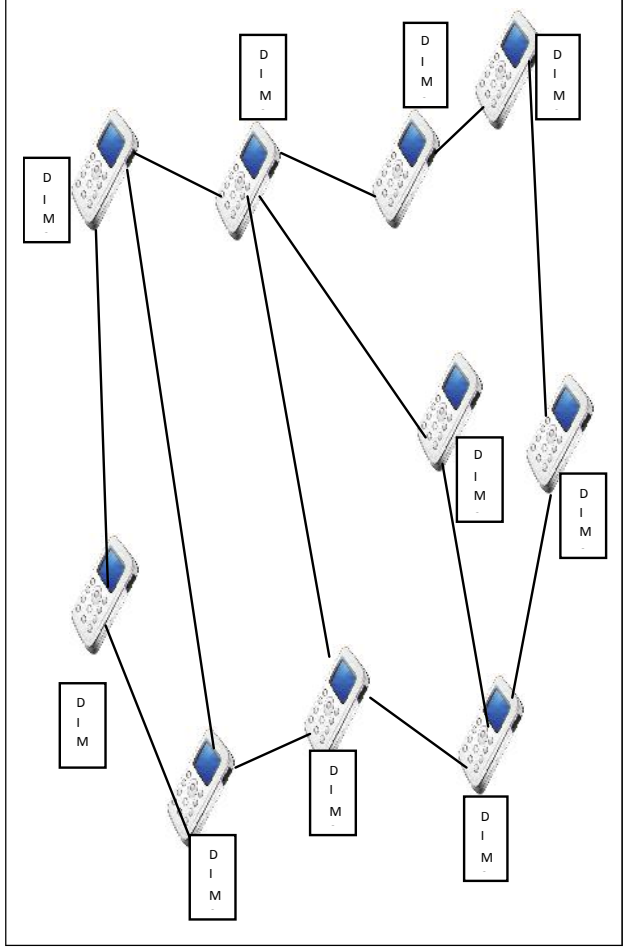


The systems differ in the way this information is spread and in the formula used to evaluate reputation value. The aim of a system for the node is to be able to find the best possible route for sending own packets and eventually to prevent misbehaving nodes from using the network. In this section, various reputation and trust-based systems as proposed in the literature for MANETs are reviewed in what follows.

Proposed Detectors for Intrusion and Malicious, Selfish Node (DIMS)

Proposed behavior based anomaly intrusion detection system intrusion detection and response systems must be both collaborative and distributed to suit the needs of mobile ad-hoc networks. In this DIMS structure as shown in Figure 4, all nodes in the MANET take part in intrusion detection and response. Each device is liable for detecting symptoms of violation locally and independently, but neighboring devices can jointly examine in a broader range.

Figure 4: DIMS Frame Work for MANET



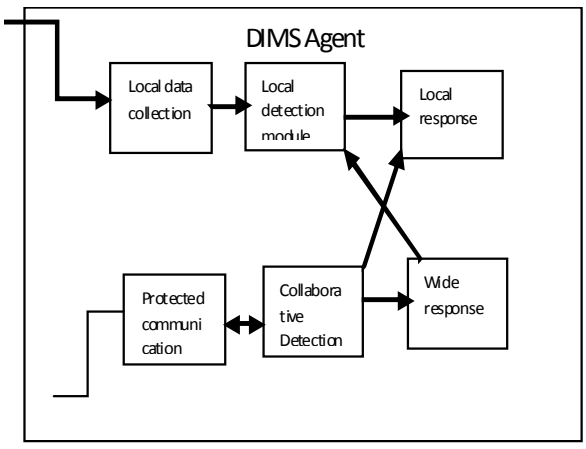
Each DIMS entity runs individually and observes local activities including systems and client activities and communication activities within the broadcast range [1]. DIMS perceives invasion from local traces and initiates appropriate response. If abnormality is discovered in the local data or if the proof is unconvincing and then a wide search is permitted, allowing neighboring DIMS agents to participate in comprehensive intrusion detection action. These individual DIMS agents collectively form the DIMS system to defend the mobile ad hoc network.

The internal units of the DIMS can be quite complex, but conceptually it can be organized into six pieces as shown in Figure 5. The data collection section is liable for collecting local activity logs and audit traces. Subsequently, the local detection module will exploit these data to detect the local anomalies. Detection schemes that require larger data sets or that need collaborations among DIMS agents will use the cooperative detection module. Invasion response deeds are furnished by both the local response and broad response modules. The local response section activates actions confined to this mobile node. For example, the DIMS agent alerts the local node. while the broad one coordinates actions among neighboring nodes such as the DIMS agents in the network selecting a remedial action. Further, it is assumed that a shielded communication unit affords a secret communication channel among DIMS units.

Methodology of Detection Systems

This section focuses on how to create anomaly detection models for mobile wireless networks. The main components of anomaly detection mechanism applied in the present research work are as follows: (1) anomaly

Figure 5: Incoming/Outgoing Traffic Traces



detection engine-this is where the captured audit data is compared to the user/network profiles stored in the profile database. (2) Reports database-this is where the normal reports of client and network behaviors are stored.

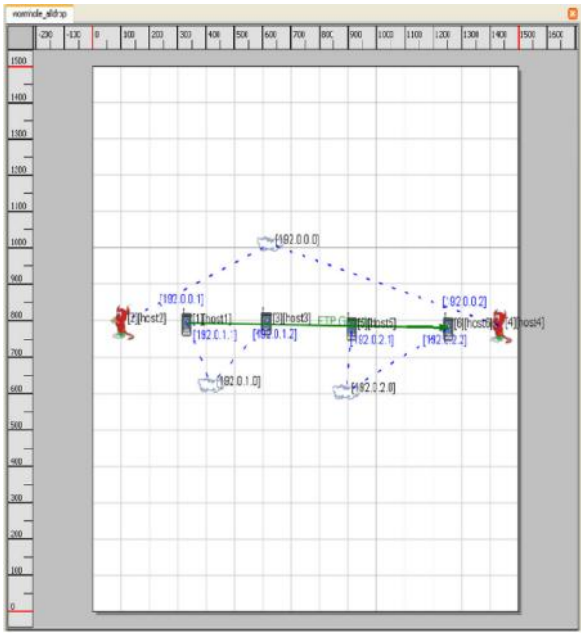
It is fairly hard to compose a complete set of network/user profiles for a MANET, due to its unique characteristics [17]. The common practice in a MANET research is to build the network/ user reports of a MANET based on certain specification applied in the network, such as routing protocol or security mechanism specification. A similar practice is applied in this research work.

The basic principle for anomaly detection is to observe attribute of normal behavior that is different from that of abnormal behavior. The detectors of DIMS are trained by using normal data to forecast what is normal in the consequent event, given the previous 'n' events. In supervising, when the genuine event is not what the detector has predicted, there is an anomaly. Using this framework, the following method for anomaly detection is employed: (a) select audit data, (b) carry out suitable data transformation according to the binary representation, (c) compute detector using training data, (d) apply the detector to test data, and (e) post-process alarms to produce intrusion reports.

Worm Hole Attack Model: Attitude Agent Intrusion Detector Systems (AAIDS)

In this present research work, wormhole attack is implemented using Qualnet simulator as shown in Figure 6. The attack scenario for the ad hoc network is briefly illustrated in this

Figure 6: Wormhole Attack Model



section. In this wormhole attack, the adversary disrupts ad hoc routing protocols using higher bandwidth and lower-latency links. Wormhole attack is more hidden in character and tougher to detect [18]. The term wormhole refers to adversary carrying information and travelling faster than anyone else. Thus, the adversary is capable of launching unusual timing attacks. Attacker can relays packets quicker than regular nodes that need a queuing delay, transmission delay and MAC contention delay [19]. A wormhole assailant digs messages collected in one place in the network over a low-latency high-bandwidth link and rebroadcasts them in a different place. This usually necessitates at least two adversarial gadgets colluding to relay packets along a speedy channel available only to the attackers, so that it can interrupt multi-hop ad hoc routing. In the presence of wormholes, the attacking nodes can selectively let routing control messages get through them. Then, the

wormhole link has a higher probability of being chosen as part of multi-hop routes due to its excellent packet delivery capability. Once the attacking nodes know they are enrouted, they can launch a black hole attack to drop all data packets or a gray hole attack to selectively drop some critical packets. A wormhole attack is implemented in three modes: (1) THRESHOLD: In this mode, wormhole drops any packet with size greater than or equal to the threshold value. It shows the wormhole tunneling function with a user defined threshold value (72 bytes in this case). (2) ALLPASS: Wormhole passes all packets irrespective of their size during this mode. It shows how wormhole passes all packets including control packets and data packets. (3) ALLDROP: In this mode, the wormhole drops all the packets irrespective of their size. It shows how the wormhole drops all the packets including control packets and data packets.

The following steps are performed to create this attack Scenario using the GUI [20]:

1. Place six nodes of the default device type and three wireless subnets on the canvas. Connect all the nodes to the corresponding wireless subnet as shown in the Figure 6.
2. To set MAC protocol for second subnet (nodes 2 and 5), go to MAC layer tab of wireless subnet properties editor and set MAC protocol to wormhole and set wormhole parameters.
   - To enable the THRESHOLD mode, set wormhole operation mode to Threshold.
   - To enable the ALLPASS mode, set wormhole operation mode to All Pass.
   - To enable the ALLDROP mode, set wormhole operation ode to All Drop.
3. Create CBR application between node 1 and node 6.

DIMS Extension for DSR, AODV and DSDV Routing Protocols

The simulated network comprises mobile nodes acting both as terminals and information relays with sufficient infrastructure for radio communication. This setup relates to an ad-hoc network that usually utilizes multi-hop routing scheme. In the present work, DSR + AAIDS, AODV + AAIDS and DSDV + AAIDS protocols have been developed. Three different simulation experiments were conducted to study the performance of DSR, AODV and DSDV routing protocols with and without DIMS extensions for the detection of wormhole based misbehaving Nodes.

DSR + AAIDS

In the first simulation scenario, AAIDS agent is incorporated among all the nodes in the ad hoc network. In DSR + AAIDS scheme, AAIDS agent is working on the top of DSR routing protocol [21]. Each of these nodes. participates in the route discovery process of the DSR routing protocol. There are two stages. During the first stage, AAIDS agent in each node studies the normal traffic pattern of DSR protocol events. This is called as learning phase. During second stage, wormhole attacks are introduced over few numbers of nodes where they acted as misbehaving nodes. Now, AAIDS agent attempts to detect anomalies by observing the change in traffic pattern. This is termed as detection phase. The method of data collection will be delineated in the subsequent Sect. C

AODV + AAIDS

In this simulation scenario, AAIDS agent is

incorporated among all the nodes in the ad hoc network. AAIDS is working on the top of AODV routing protocol [22]. In the learning first phase, AAIDS agent in each node studies the normal traffic pattern of AODV protocol events. During second phase, wormhole attacks were introduced over few observing the change in traffic pattern.

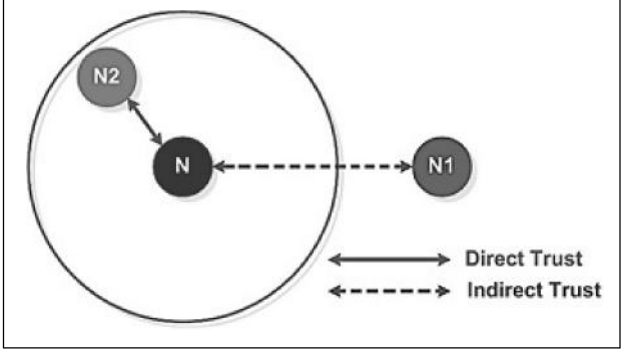
COMPANION-BASED ROUTING PROTOCOL (CRP)

In CRP, trust of the nodes is determined by sending challenges and sharing friends' lists. The proposed algorithm is divided into four stages: Challenge your neighbor, Rate friends, Share friends and Route through friends. Challenges are sent to authenticate the nodes. Nodes which complete the challenge are put into the friend list and otherwise they are put into the question mark list. In rate friends stage friends rating is done on the basis of the amount of data they transmit and rating obtained by other friends.

Node's Trust Value Calculation

Measuring the trust value of a node is always a challenging problem [10, 11]. A node's trustworthiness ito the quality of services it provides to others. If the quality of a service can be objectively measured, then an entity's trustworthiness for that service is called objective trust. Most of the previous researches used the approach of subjective trust. They classified the trust relation as a direct and an indirect relation, Figure 7 shows the type of trust relationships. Each node has a direct trust relation with the nodes located inside its communication range (neighbors); the direct trust relation is computed by monitoring the behavior of the neighbors in the routing

Figure 7: Type of Trust Reltionships



process. On the other hand, the indirect trust relation is concerned with the other nodes located outside the node's communication range (non-neighbors); a useful method to compute the indirect trust relation is flooding the network with request messages and waiting replies. Evaluating the direct and indirect trust relation consumes both bandwidth and energy, delays the route discovery process and complicates the routing process due to the additional computational overhead.

The development of our trust value calculation method is based on the Secure and Objective Reputation based Incentive (SORI) basic scheme [23]. In that scheme, neighbor monitoring is used to collect information about the packet-forwarding behavior of the neighbors. Due to the promiscuous mode that they assume, a node is capable of overhearing the transmissions of its neighbors. With this capability, a mobile node N can maintain a neighbor node list (denoted by NNLN) which contains all of its neighbor nodes that node N learns of by overhearing. In addition, node N keeps track of two numbers, for each of its neighbor (denoted by M), as below. RFN (M) (Request-for-Forwarding): The total number of packets that node N has transmitted to node

M for forwarding. HFN (M) (Has-Forwarded): The total number of packets that have been forwarded by node M and noticed by node N.

With the fore-mentioned neighbor monitoring, a node could build a record of the reputation of its neighboring nodes (direct trust relationship). Reputation propagation is employed to have neighbors share the reputation information (indirect trust relationship).

Self Monitoring Node

The reputation propagation works as follows:

1. Each node N periodically updates its LERN (M) for each neighbor node M based on the changes of RFN (M) and HFN (M), and it broadcasts the updated record to its neighborhood if CN (M) has significantly changed.
2. Node N uses its LERN (M) and LERi (M) (where i is in the NNLN) to calculate its Overall Evaluation Recorded node M (denoted by OERN(M)) as [24]:

$$\mathrm{OER}_N(M) - \frac{\sum i \in NNL_N \cup \{N\}, i \neq X, \lambda_N(i).C_i(M).G_i(M)}{\sum k \subset NNL_N \cup \{N\}, k \neq M, \lambda_N(k).C_k(M)}$$

The trust value basic scheme calculation has several drawbacks. (1) Increased node's power consumption because it assumes that each node operates in a promiscuous mode to monitor its neighbors continually. (2) Flooding the network by broadcasting the updated evaluations consumes the network limited bandwidth. (3) The broadcasted evaluation records may come from misbehaving nodes which leads to wrong results. (4) Taking into consideration the credibility of node i which broadcasts its evaluation record about node X when calculating OER(X) leads to computational overhead. (5) It does not take into account a node's "selective forwarding" behavior, where it only forwards small packets while selectively discarding larger ones.

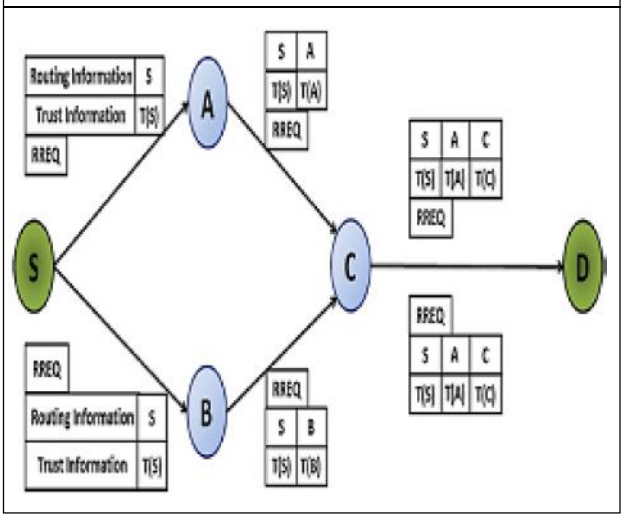
$$Trust\_Value\,(M) = \frac{HF(M) * Pkt\_Size(HF(M))}{RF(M) * Pkt\_Size(RF(M))}$$

Trust Values Propagation

In order to disseminate the trust information without flooding the network with request messages, ATDSR depends on transferring the trust values of nodes through the Route Request packets as shown in Figure 8. In addition to the routing information, each Route Request (RREQ) packet contains a trust record in which is accumulated a record of the sequence of hops taken by the RREQ packet as it is propagated through MANETs during this Route Discovery process.

For each node acting as a forwarder during the Route Discovery process, its routing agent ROA is responsible for appending the computed trust value of that node to the RREQ packet that was sent by the preceding node. In this manner, when a RREQ packet is sent, it

Figure 8: Trust Value Propagation Through RREQ Packets



carries the trust information about each forwarding node.

PERFORMANCE EVALUATION: INTRUSION AND MALICIOUS, SELFISH NODE

Simulation Environment

The data packet size was 512 bytes. The wireless transmission range of each node was Tr = 250 m. In the simulations, Nt = 100 mobile nodes randomly distributed over a 700 (m) by 500 (m) flat area. The source and the destination nodes were randomly chosen among all nodes in the network. The total simulation time was 900 s. For each experiment, 20 simulations were run to obtain the average values. Both UDP and TCP traffics have been simulated to evaluate the performance of our model. A random waypoint mobility model [21] was assumed with a maximum speed of Vm = 10-50 m/s and a pause time of 0 s. The mobility scenarios were generated by the "random trip" generic mobility model. The Constant Bit Rate (CBR) traffic model was used. Each simulation included 50 CBR sessions, each CBR session generated four packets per second.

Routing Misbehavior Problem

In this section, the routing misbehavior problem is illustrated in the context of the DSR protocol; the following notations are used while describing the problem caused by routing misbehavior: Pr The ratio of misbehaving routes Pm The ratio of misbehaving nodes In order to demonstrate the adverse effect of routing misbehavior, we compute the ratio of misbehaving routes.

Figure 9: Simulation Result with Varying No of Malicious Nodes

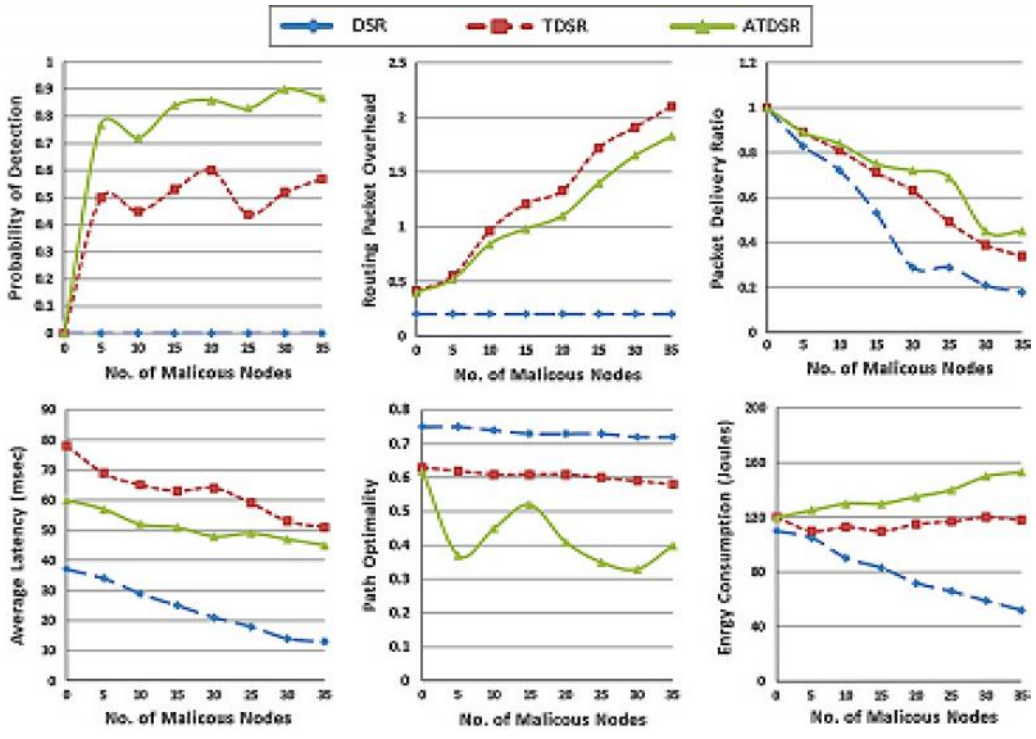
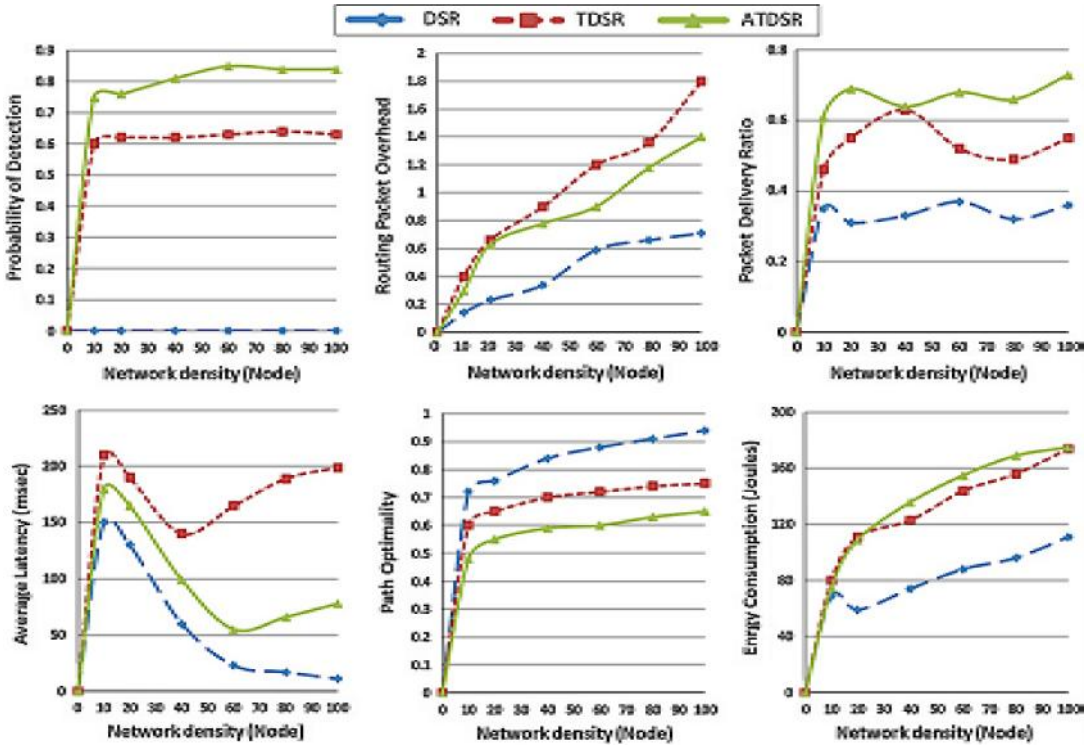


Figure 10: Simulation Results with Varying Number Nodes



Simulation Results and Analysis

This section presents our simulation methodology. To examine ATDSR, we compared it with that the standard DSR [17] protocol and Trusted DSR (TDSR) [22]. A total of three simulations were conducted to evaluate the performance of ATDSR under varying number of malicious nodes, mobility and node density. The parameters mentioned above in the simulation environment are common to all three simulations. To evaluate the performance of the proposed scheme, the following metrics are adopted [22]: Packet Delivery Ratio (PDR)c The ratio between the number of packets received by the destination nodes to the number of packets sent by the source nodes Routing Packet Overhead (RO) The ratio between the total number of control packets generated to the total number of data packets received during the simulation time Average Latency (AL) The mean time taken by the packets to reach their respective destinations (in milliseconds).

PERFORMANCE EVALUATION: WORM HOLE ATTACK MODEL

Qualnet v 4.5 simulator has been used to analyze AAIDS in detecting wormhole based misbehavior for the underlying dynamic source routing (DSR), ad-hoc on-demand distance vector (AODV) and destination sequence distance vector (DSDV) routing protocols. Since AAIDS works as an extension technique for the DSR, AODV and DSDV routing protocols, the performance of the AAIDS scheme is actually the performance of the DSR + AAIDS, and DSDV + AAIDS. In addition to

that, effectiveness of DSR + AAIDS, AODV+ AAIDS and DSDV + AAIDS are compared with the existing DSR + HNSA to improve the network performance. Simulation results are based on the following metrics: (1) detection rate, (2) false alarm rate, (3) packet delivery ratio, (4) routing overhead.

CONCLUSION

The routing protocol is critical to MANET's performance, there for security is crucial. A Comprehensive review of some important research focusing on Trusted routing protocol of providing security with a critical evaluation of their strength and weakness are also presented. CRP depends on self monitoring of each node to find out its trust value. Attitude Agent Intrusion Detector Systems (AAIDS), which obtained information available from the routing protocol for intrusion detection purposes. These detectors are capable of tracing an intrusion by observing deviations from the normal or expected behavior of nodes.

REFERENCES

1. Azandaryani A H M and Meybodi M R (2009), "A Learning Automata Based Artificial Immune System for Data Classification", in Proceedings of IEEE Computer Conference, pp. 530-535.
2. Buchegger S and Boudec L (2002), "Performance Analysis of the CONFIDANT Protocol", in Proceedings of the 3rd ACM International Symposium on Mobile Ad Hoc Networking & Computing, pp. 226-236, Lausanne, Switzerland.
3. Dasgupta D and Gonzalez F (2002), "An Immunity Based Technique to Characterize Intrusions in Computer Networks", *IEEE Transactions on Evolutionary Computation*, Vol. 3, pp. 281-291.
4. De Castro L N and Timmis J (2002), "An Introduction to Artificial Immune Systems: A New Computational Intelligence Paradigm", in Proceedings of IEEE Congress on Evolutionary Computation, pp. 699-674.
5. Dhurandher S K and Mehra V (2009), "Multi-Path and Message Trust-Based Secure Routing in ad hoc Networks", in *Proceedings International Conference Advances in Computing, Control and Telecomm*. *Technologies*, pp. 189-194, Trivandrum, Kerala.
6. Forrest S, Perelson A S, Allen L and Cherukuri R (1994), "Self-Nonself Discrimination in a Computer", in Proceedings of the IEEE Symposium on Research in Security and Privacy, pp. 202-212, IEEE Computer Society Press.
7. Gonzalez F A and Dasgupta D (2003), "Anomaly Detection Using Real-Valued Negative Selection", *Journal Genetic Programming and Evolvable Machines*, Vol. 4, pp. 383-403.
8. He D *et al.* (2012), "Re Trust: Attack-Resistant and Lightweight Trust Management for Medical Sensor Network", *IEEE Transactions on Information Technology in Biomedicine*, Vol. 16, No. 4, pp. 623-632.
9. Johnson D and Maltz D (1996), "Dynamic Source Routing in ad hoc Wireless Networks", in I A Korth (Ed.), *Mobile Computing*, Vol. 353, pp. 153-181, Norwell, Kluwer.

10. Lau F, Rubin S H and Smith M H (2000), "Distributed Denial of Service Attacks", in Proceedings of the IEEE International Conference on Systems, Man, and Cybernetics, pp. 2275-2280.

11. Li X, Jia Z, Zhang P, Zhang R and Wang H (2010), "Trustbased On-Demand Multipath Routing in Mobile ad hoc Networks", *Information Security*, *IET*, Vol. 4, No. 4, pp. 212-232.

12. Li X, Lyu M R and Liu J (2004), "A Trust Model Based Routing Protocol for Secure ad hoc Networks", in Proceedings of IEEE Aerospace Conference, pp. 1286-1295, Big Sky, Montana, USA.

13. Liu K and Deng J (2007), "An Acknowledgment-Based Approach for the Detection of Routing Misbehavior in MANETs", *IEEE Transactions on Mobile Computing*, Vol. 6, No. 5, pp. 536-550.

14. Maleknasab M and Bidaki M (2013), "Trust-Based Clustering in Mobile ad hoc Networks: Challenges and Issues", *International Journal of Security and Its Applications*, Vol. 7, No. 5, pp. 321-342.

15. Marti S, Giuli T J, Lai K and Baker M (2000), "Mitigating Routing Misbehavior in Mobile ad hoc Networks", in Proceedings of Mobile Computing and Networking (MobiCom'00), pp. 255-265.

16. Michiardi P and Molva R (2002), "CORE: A Collaborative Reputation Mechanism to Enforce Node Cooperation in Mobile ad hoc Networks", in Proceedings of the 6th IFIP Conference on Security Communications, and Multimedia, pp. 107-121, Portoroz, Slovenia.

17. Ou C-M (2012), "Host-Based Intrusion Detection Systems Adapted from Agent-Based Artificial Immune Systems", *Journal of Neuro Computing*, Vol. 88, pp. 78-86.

18. Pirzada A A and McDonald C (2006), "Reliable Routing in MANETs Using Direct Trust Mechanisms", in *Advances in Ad Hoc and Sensor Networks*, Ch. 6, pp. 133-159, Springer, Berlin.

19. Pirzada A A, McDonald C and Datta A (2007), "Dependable Dynamic Source Routing Without a Trusted 3rd Party", *Journal of Research and Practice in Information Technology*, Vol. 39, No. 1, pp. 71-85.

20. Rahman A A and Hailes S (1997), "A Distributed Trust Model", in Proceedings of the ACM New Security Paradigms Workshop, pp. 48-60, Cumbria, UK.

21. Sarafijanovic S and Le Boudec J-Y (2005), "An Artificialimmune System Approach with Secondary Response for Misbehavior Detection in Mobile ad hoc Networks", *IEEE Transactions on Neural Networks*, Vol. 5, pp. 1076-1087.

22. Sompayrac L M (2003), *How the Immune System Works*, 2nd Edition, Blackwell, Oxford.

23. Yang H, Luo H, Ye F, Lu S and Zhang L (2004), "Security in Mobile ad hoc Networks: Challenges and Solutions", *IEEE Wireless Communications*, Vol. 11, No. 1, pp. 38-47.

24. Zhan G, Shi W and Deng J (2012), "Design and Implementation of TARF: A Trust-Aware Routing Framework for

WSNs", *IEEE Transactions on Dependable and Secure Computing*, Vol. 9, No. 2, pp. 184-197.

25. Zhang Y, Lee W and Huang Y (2003), "Intrusion Detection Techniques for Mobile Wireless Networks", *ACM Wireless Networks Journal*, Vol. 5, pp. 545-556.