Journal of Computer Science 7 (12): 1854-1858, 2011
ISSN 1549-3636

# System of One to Three Umpire Security System for Wireless Mobile Ad hoc Network

[1]C. Rajabhushanam and [2]A. Kathirvel
[1]Department of CSE, Tagore Engineering College, Chennai, India
[2]Department of CSE, Karpaga Vinayaga College of Engineering and Technology, India

**Abstract: Problem statement:** A Mobile Ad Hoc Network (MANET) is a self-created self-organized and self-administering set of nodes connected via wireless links without the aid of any fixed infrastructure or centralized administrator. Protecting the network layer from malicious attacks is an important and challenging issue in both wired and wireless networks and the issue becomes even more challenging in the case of MANET. **Approach:** In this study we propose an Umpiring System (US) that provides security for routing and data forwarding operations. We present three US models-Single (one) Umpiring System (SUS), Double Umpiring System (DUS) and Triple Umpiring System (TUS). In the umpiring system, each paricipating node of the system will have different roles to play; some of the nodes will be doing traditional operations of routing and packet forwarding, while some others will be monitoring the behaviour of designated nodes. If any misbehavior is noticed umpires immediately flag off the guildy node. **Results:** We find that. Throughput with single umpire system is greater than DUS and TUS. From throughput and energy point of view SUS is the best. But both false positives and false negatives are lower with TUS, indicating it is a better detection system. **Conclusion:** We envisage that our system can profitably be used in civilian situations where invariably nodes are lean and energy starved.

**Key words:** Malicious nodes, Triple Umpiring System (TUS), Umpiring System (US), Double Umpiring System (DUS), Mobile Ad Hoc Network (MANET), wireless networks, centralized administrator

## INTRODUCTION

A Mobile Ad Hoc Network (MANET) is a self-created self-organized and self-administering set of nodes connected via wireless links without the aid of any fixed infrastructure or centralized administrator. Each node moves and operates in a distributed peer-to-peer mode, generating independent data and acting as a router to provide multi-hop communication. MANET is ideally suited for potential applications in civil and military environments, such as responses to hurricane, earthquake, tsunami, terrorism and battlefield conditions. Security is an important aspect in such mission critical applications.

In this study we tackle the problem of securing the network layer operations from malicious nodes. Malicious nodes may disrupt routing algorithms by transmitting a false hop count; they may drop packets, route the packets through unintended routes and so on. Our work rests on the foundations of two excellent systems already proposed: The twin systems of watchdog and pathrater (Marti *et al*., 2000) and SCAN (Yang *et al*., 2006). A brief look at each one of them is in order.

Marti *et al*. (2000) introduced two extensions to the Dynamic Source Routing Protocol DSR to mitigate the effect of routing misbehaviors-watchdog and pathrater. The watchdog identifies misbehaving nodes while the path rater avoids routing packets through these nodes. When a node forwards packets the node's watchdog verifies that the next node in the path also forwards the packet. The watchdog does this by listening promiscuously to the next hop transmissions. If the next node doesn't forward the packet then it is misbehaving. The watchdog detects the misbehavior and sends a message to the source, notifying it of the misbehaving node.

In SCAN (Yang *et al*., 2006), each node monitors the routing and packet-forwarding behavior of its neighbors and independently detects the existence of malicious nodes in its neighborhood. This is made possible because of wireless nature of the medium and all the involved nodes are within each other's transmission. In order to enable cross-checking they have modified AODV protocol and added a new field next_ hop in the routing messages so that each node can correlate the overheard packets accordingly.

**Corresponding Author:** C. Rajabhushanam, Department of CSE, Tagore Engineering College, Chennai, India

While each node monitors it neighbors independently all the nodes in the neighborhood collaborate to convict a malicious node. An agreement between a minimum of k neighboring nodes is required for convicting a malicious node. Once its neighbors convict a malicious node the network reacts by depriving it of its right to access the network. In SCAN each node must possess a valid token in order to interact with other nodes. They have used asymmetric key cryptography to prevent forgeries of tokens. A group of nodes (minimum-k) can collaboratively sign a token, while no single node can do so. Further each node has to get its token renewed periodically by its neighbors. A node which behaves continuously in a good manner can get its token renewed at less frequent intervals as compared to a fresh entrant node.

Our umpiring system has been strongly influenced by the above two schemes. In our system all the active nodes have different roles to play: Routing and packet forwarding and monitoring as in SCAN. However, unlike SCAN only designated nodes-umpires monitor the behaviour of nodes, in Single Umpiring System (SUS) and Double Umpiring System (DUS) (Kathirvel and Srinivasan, 2011a; 2011b and Kathirvel and Rajabushanam, 2011). In Triple Umpire System (TUS) the nodes in the active path play dual role of routing and monitoring as in watchdog. We also exploit promiscuous hearing functionality as done by both SCAN and watchdog. We have adopted the token concept from SCAN. Token is a pass or validity certificate enabling a node to participate in the network. It contains two fields: Nodeid and status bit; nodeID is considered to be immutable. Initially the status bit of all participating nodes is set as zero indicating “green flag” with freedom to participate in all network operations. It is assumed that a node cannot change its status bit. In SUS when an umpiring node finds the node it is monitoring as misbehaving, it sends a M-Error message to the source and malicious node’s status bit is changed using M-Flag message and set to 1 indicating “red flag”. With “red flag” on the culprit node is prevented from participating in the network. In DUS and TUS the decision is made by two and three umpires, respectively in conjection.

Our objective is designing the security system is to keep the overhead as minimum as possible while optimizing the throughput. We do not use encryption or key algorithms as done by SCAN. We find that token issuing and token renewals and broadcasts to announce convictions create very large communication overheads and also degrade energy performance, which SCAN has completely over looked. There is no token renewal feature in our system. In our system all the nodes are pre issued with green tokens. They continue to enjoy the status until any umpire finds the node misbehaving and sends the M-Error and M-Flag messages and red flag is set.

Just like SCAN in order to facilitate cogent promiscuous hearing we have used “next_hop” field with our AODV implementation. Our umpiring system can detect any false reporting of hop count during the route reply process RREP. In watchdog detection of malicious action is by a single node while in SCAN it is done by a set of neighbors. In our system the designated umpiring nodes in their role as umpires carry out both detection and conviction.

**Umpiring system security model:** In the umpiring system each node is issued with a token at the inception. The token consists of two fields: NodeID and status. NodeID is assumed to be unique and deemed to be beyond manipulation; status is a single bit flag. Initially the status bit is preset to zero indicating a green flag. The token with green flag is a permit issued to each node, which confers it the freedom to participate in all network activities.

Each node in order to participate in any network activity, say Route Request RREQ, has to announce it’s token. If status bit is “1” indicating “red flag” protocol does not allow the node to participate in any network activity.

We propose three models for the umpiring system - Single Umpiring System (SUS), Double Umpiring System (DUS) and Triple Umpiring System (TUS). We go on to describe each of these systems presently (Kathirvel and Srinivasan, 2011a, 2011b; and Kathirvel and Rajabushanam, 2011).

**Single Umpiring System (SUS):** In SUS, an umpire is appointed corresponding to each node in the active path, excluding source and destination is illustrated in Fig. 1. Thus if there are m intermediate nodes in the active path there will be m umpires. In Fig. 1 Ni-1, Ni, Ni+1 are the nodes in the active path; Ui-1, Ui, Ui+1 are corresponding umpires. Umpire Ui can tell correctly whether node Ni is forwarding the packet to Ni+1 correctly as received from Ni-1 or not, by promiscuously hearing Ni’s transmissions. During route reply process RREP, Ui can again verify that information transmitted by Ni+1 is correctly forwarded by Ni.

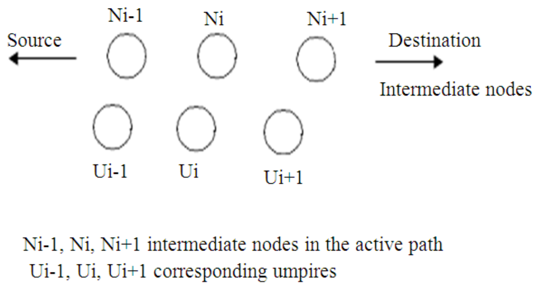
Source
Ni-1
Ni
Ni+1
Destination
Intermediate nodes
Ui-1
Ui
Ui+1
Ni-1, Ni, Ni+1 intermediate nodes in the active path
Ui-1, Ui, Ui+1 corresponding umpires

Fig. 1: Single umpiring system model

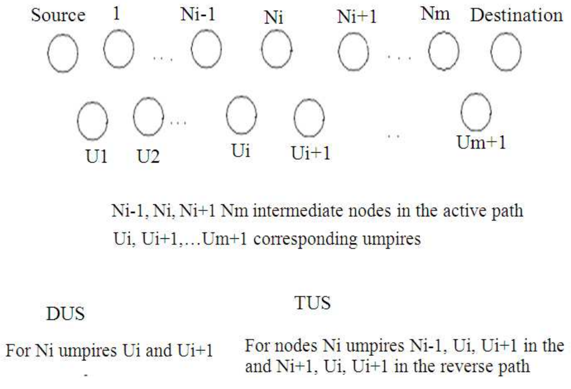
Source
1
Ni-1
Ni
Ni+1
Nm
Destination
U1
U2
Ui
Ui+1
Um+1
Ni-1, Ni, Ni+1 Nm intermediate nodes in the active path
Ui, Ui+1,…Um+1 corresponding umpires
DUS
TUS
For Ni umpires Ui and Ui+1
For nodes Ni umpires Ni-1, Ui, Ui+1 in the and Ni+1, Ui, Ui+1 in the reverse path

Fig. 2: Double and triple umpiring systems

When Ni is found to be misbehaving-say dropping packets or changing Hop_count or sequence number, Ui sends a M-ERROR message to the source and sets the status bit of guilty node Ni to “1” indicating red flag by M-Flag message.

**Double Umpiring System (DUS):** In Double Umpiring System (DUS) (Fig. 2) each intermediate node in the active path is monitored by two umpires. Thus umpire Ui monitors the behavior of two nodes Ni-1 and Ni. Ui+1 monitor Ni and Ni+1 and so on. In order to enable this Ui is selected such that it is within the communication range of both Ni-1 and Ni. Further adjacent umpires can communicate with each other. There are ‘m’ intermediate nodes and (m+1) umpires.

If node Ni misbehaves, umpires Ui and Ui+1 is conjunction decide and the status bit of Ni is changed to 1.

**Triple Umpiring System (TUS):** Triple Umpiring System can be explained again with reference to Fig. 2. For node Ni, Ni-1, Ui and Ui+1 will be umpires in the forward path and Ni+1, Ui and Ui+1will be umpires in the reverse path. If Ni behaves as determined by all the umpires the status bit of node Ni is set as one (Kathirvel and Srinivasan, 2011a, 2011b; and Kathirvel and Rajabushanam, 2011).

## RESULTS AND DISCUSSION

We use a simulation model based on QualNet 4.5 in our evaluation (Kathirvel and Srinivasan, 2011a; 2011b and Kathirvel and Rajabushanam, 2011). Our performance evaluations are based on the simulations of 100 wireless mobile nodes that form a wireless ad hoc network over a rectangular (1500×600 m) flat space. The MAC layer protocol used in the simulations was the Distributed Coordination Function (DCF) of IEEE 802.11. The performance setting parameters are given in Table 1 (Kathirvel, 2010).

Before the simulation we randomly selected a certain fraction, ranging from 0-40% of the network population as malicious nodes. We considered only two attacks-modifying the hop count and dropping packets. Each flow did not change its source and destination for the lifetime of a simulation run.

We have done three studies corresponds to 10 flows with flows between 10 different source-destination pairs. Study I corresponds to SUS, Studies II and III are corresponds to DUS and TUS respectively.

Our experiments are based on four important parameters:

**Throughput:** In the world of MANET, packet delivery ratio has been accepted as a standard measure of throughput. Packet delivery ratio is nothing but a ratio between the numbers of packets received by the destinations to the number of packets sent by the sources. We present in Table 2 the packet delivery ratios in the case of 30 percentage of malicious node, with node mobility varying between 0-20 m sec.

From Table 2 the following conclusions can be drawn:

- In general packet delivery ratio decreases as mobility and percentage of malicious nodes increase
- For example, in the case of SUS packet delivery ratio drops from 71.23-63.52% as the node mobility increases to 20 m sec
- SUS has higher throughput in all cases compared to DUS and TUS. From the above study we conclude that SUS fairs best as compared to other two models, from the point of view of throughput

**Failure to deduct (false negatives) probability:** False Negatives Probability can be defined as:

False Negatives Probability = number of malicious nodes left undetected/total number of malicious nodes

From Table 3 the following conclusions can be drawn:

- In general false negative probability decreases as mobility increases
- As we move from SUS to TUS, there is a decrease in false negative probability

From the above results we conclude that TUS has the least false negative probability when compared with DUS and TUS.

**False accusation (false positives) probability:** It can be seen that lowest false positives probability is obtained with TUS (Refer Table 4). In other words innocent node booking is minimum with TUS.

Table: 1 Parameters setting

| | |
|---|---|
| Simulation time | 1500 sec |
| Propagation model | two ray ground reflection |
| Transmission range | 250m |
| Band width | 2 Mbps |
| Movement model | random way point |
| Pause time | 0 sec |
| Traffic type | CBR (UDP) |
| Payload size | 512 bytes |
| Number of flows | 10/20 |

Table 2: Packet delivery ratios for the 3 studies

| | Malicious nodes = 30% | | |
|---|---|---|---|
| Mobility (M sec) | SUS | DUS | TUS |
| 0 | 73.23 | 72.84 | 70.95 |
| 5 | 68.86 | 64.18 | 61.51 |
| 10 | 65.41 | 61.11 | 58.42 |
| 15 | 64.38 | 60.88 | 58.26 |
| 20 | 63.52 | 59.18 | 56.29 |

Table 3: False negatives probability for the 3 studies

| | Malicious nodes = 30% | | |
|---|---|---|---|
| Mobility (M sec) | SUS | DUS | TUS |
| 0 | 0.1974 | 0.1852 | 0.1731 |
| 5 | 0.1594 | 0.1513 | 0.1471 |
| 10 | 0.0916 | 0.0749 | 0.0618 |
| 15 | 0.1091 | 0.0988 | 0.0871 |
| 20 | 0.1007 | 0.0918 | 0.0873 |

Table 4: False positives probability

| | Malicious nodes = 30% | | |
|---|---|---|---|
| Mobility (M sec) | SUS | DUS | TUS |
| 0 | 0.0000 | 0.0000 | 0.0000 |
| 5 | 0.0136 | 0.0116 | 0.0091 |
| 10 | 0.0592 | 0.0471 | 0.0354 |
| 15 | 0.0764 | 0.0692 | 0.0511 |
| 20 | 0.0816 | 0.0748 | 0.0612 |

Table 5: Communication overhead

| | Malicious nodes = 30% | | |
|---|---|---|---|
| Mobility (M sec) | SUS | DUS | TUS |
| 0 | 15254 | 15305 | 15390 |
| 5 | 16110 | 16160 | 16206 |
| 10 | 16930 | 17046 | 17151 |
| 15 | 17848 | 17936 | 18025 |
| 20 | 18523 | 18642 | 18713 |

Table 6: Throughput and communication overhead of 30% malicious nodes with plain AODV

| Mobility (M sec) | 0 | 5 | 10 | 15 | 20 |
|---|---|---|---|---|---|
| Throughput | 70.44 | 45.18 | 37.89 | 32.55 | 32.0700 |
| Comm overhead | 14136.00 | 14603.00 | 15082.00 | 15580.00 | 16082.0 |

**Communication overhead** Communication overhead can be evaluated based on the number of transmissions of control messages like RREQ, RREP, RERR, M_ERROR and M-Flag messages in the umpiring system. We present the communication overhead details in Table 5. We find that communication overhead increases with mobility and SUS has the lowest communication overhead.

**Analysis of results:** We present the plain AODV results in Table 6. We find that all the 3 umpiring systems SUS, DUS and TUS yield much higher output as compared to plain AODV. The increase in communication overhead ranges from 7.9% (SUS, 0 m sec mobility) to 16.4 % (TUS 20 m sec mobility).

Clearly with DUS and TUS, with more umpires involved in detection, false negatives and false positives probabilities decrease. Thus with TUS we have better rounding up of malicious nodes.

**Literature work:** The Key Distribution Center (KDC) architecture is the main stream in wired network because KDC has so many merits. Efficient key management, including key generation, storage, distribution and updating. The lack of Trusted Third Party (TTPs) key management scheme is a big problem in ad hoc network(Banerjee and Dutta, 2010, Maalla *et al*., 2009; Kaabneh *et al*., 2009, Elfaki *et al*., 2011, Natsheh and Buragga, 2010) (Kathirvel and Sivaraman, 2010). All the above schemes only try to protect the system from the attacker, but not bother about quarantining attackers. The twin systems of watchdog and pathrater (Marti *et al*., 2000) not only detect the mischievous nodes but also prevent their further participation in the network. SCAN (Yang *et al*., 2006) also has similar action, but is more comprehensive, in the sense not only packet dropping but also other misbehaviors like giving wrong hop count are covered.

## CONCLUSION

An umpiring system for security for mobile ad hoc network has been proposed. We have presented experimental results for all the 3 systems. We find that Throughput with single umpire system is greater than DUS and TUS. From throughput and energy point of view SUS is the best. But both false positives and false negatives are lower with TUS, indicating it is a better detection system. We envisage that our system can profitably be used in civilian situations where invariably nodes are lean and energy starved. Further research work is in progress.

## REFERENCES

Maalla, A., C. Wei and H.J. Taha, 2009. Optimal power multicast problem in wireless mesh networks by using a hybrid particle swarm optimization. Am. J. Applied Sci., 6: 1758-1762. DOI: 10.3844/ajassp.2009.1758.1762

Banerjee, A. and P. Dutta, 2010. Link stability and node energy conscious local route-repair scheme for mobile ad hoc networks. Am. J. Applied Sci., 7: 1139-1147**.** DOI: 10.3844/ajassp.2010.1139.1147

Natsheh, E. and K. Buragga, 2010. Density based routing algorithm for spare/dense topologies in wireless mobile ad-hoc networks. Am. J. Eng. Applied Sci., 3: 312-319. DOI: 10.3844/ajeassp.2010.312.319

Kathirvel, A. and P. Sivaraman, 2010. Double umpiring system for ad hoc wireless mobile network security. Int. J. Forensic Comput. Sci., 1: 22-29.

Kathirvel, A. and R. Srinivasan, 2011a. ETUS: An enhanced triple umpiring system for security and performance improvement of mobile ad hoc networks.. Int J. Network Management, 21: 341-359. DOI: 10.1002/nem.761

Kathirvel, A. and R. Srinivasan, 2011b. ETUS: An enhanced triple umpiring system for security and robustness of mobile ad hoc networks. Int. J. Commun. Networks and Distributed Syst. Inderscience, 7: 153-187. DOI: 10.1504/IJCNDS.2011.040983

Kathirvel, A. and Rajabushanam, C, 2011c. Survey of wireless manet application in battlefield operations. Int. J. Adv. Comput. Sci. Appl., 2: 50-58.

Kaabneh, K., A. Halasa and H. Al-Bahadili, 2009. An Effective location-based power conservation scheme for mobile ad hoc networks. Am. J. Applied Sci., 6: 1708-1713. DOI: 10.3844/ajassp.2009.1708.1713

Marti, S., T.J. Giuli, K. Lai and M. Baker, 2000. Mitigating routing misbehavior in mobile ad hoc networks. Stanford University.

Elfaki, M.A., H. Ibrahim, A. Mamat and M. Othman, 2011. Collaborative caching architecture for continuous query in mobile database. Am. J. Econ. Bus. Admin., 3: 33-39.

Yang, H., J.Shu, X. Meng and S. Lu, 2006. SCAN: Self-Organized Network-Layer Security in Mobile ad hoc networks. IEEE J. Select Areas Commun., 24: 261-273. DOI: 10.1109/JSAC.2005.861384