Secured Reliable Multipath Routing Protocol (SRMRP) using Trust Computation and Carrier Sense Multiple Access with Collision Intimation (CSMA/CI) for Heterogeneous IP-based Mobile Ad-hoc Networks

B.Narasimhan
Assistant Professor
Department of Computer Technology
Dr. N. G. P. Arts and Science College
(Affiliated to Bharathiar University)
Coimbatore – 641 048

R.Vadivel
Assistant Professor
Department of Information Technology
School of Computer Science and Engineering
Bharathiar University
Coimbatore – 641 046

ABSTRACT

This paper proposes Secured Reliable Multipath Routing Protocol (SRMRP) using Distributed Trust Computation and Carrier Sense Multiple Access with Collision Intimation for Distributed Heterogeneous Mobile Ad-hoc Networks. This research aims at two main objectives. The first objective is to make the communication secured against attacks. For achieving this reference based trust security mechanism is proposed. The next objective is to provide reliable data communication in heterogeneous mobile ad hoc network. For achieving this adaptive carrier sense multiple access with collision intimation mechanism is employed. The simulations are done in NS2. This paper concerns much about real time mobile ad hoc networks i.e., heterogeneous natured. Hence we have simulated the mobile nodes with different capabilities such as transmission range, channel capacity and battery power. Extensive simulation results prove that our proposed SRMRP achieves better reliability in terms of increased throughput and packet delivery ratio. The security performance metrics such as the number(s) of detected malicious nodes and normalized control bytes are taken and SRMRP achieves better results when compared to existing AOMDV routing protocol.

Keywords

Mobile Ad hoc Networks, Multipath Routing, Trust Computation, Carrier Sense Multiple Access with Collision Intimation, Heterogeneous MANETs, IP Based MANETs

1. INTRODUCTION

A Mobile ad hoc network are infrastructure less networks which is a collection of mobile nodes that forms a temporary network without the help of centralized administration or standard support devices regularly available in conventional networks. A mobile ad hoc network which is a kind of wireless networks have the ability to establish networks at anytime, anywhere to own the assurance of the future. These mobile ad hoc networks do not depend on inappropriate hardware for the reason that it makes them ideal candidate for rescue and emergency operations. The ingredient wireless mobile nodes of these network build, operate and maintain these networks. Each wireless mobile node asks the help of its neighboring nodes to forward packets because these nodes usually have only a limited transmission range. A homogeneous ad hoc network suffers from poor scalability because the network performance is degraded quickly as the number of nodes increases. The nodes are usually heterogeneous in realistic ad hoc networks. For instance, in a battlefield network, portable wireless devices are carried by soldiers, and more powerful and reliable communication devices are carried by vehicles, tanks, aircraft, and satellites and these devices/nodes have different communication characteristics in terms of transmission power, data rate, processing capability, reliability, etc. Such heterogeneous networks nodes are portable to transmit at different power levels and thus cause communication links of varying ranges. Conventional routing protocols are held in order to launch routes between nodes which are more than a single hop. The capability to sketch routes in spite of a dynamic topology is the unique feature of these protocols. These protocols can be classified into three main types: Reactive (On-demand), Proactive (Table-driven) and hybrid. Evaluating the routes continuously within the network is done by proactive protocols, so when a packet needs to be forwarded the route is already known and can be immediately used. Reactive protocols appeal to a route determination procedure on demand only. Hybrid protocols are the combination of reactive and proactive routing mechanism. There are two main challenges in design and development of routing protocols for mobile ad hoc network. They are security, and Reliability. For overcoming those challenges, this paper portraits secured reliable multipath routing protocol (SRMRP) using carrier sense multiple access with collision intimation and distributed trust computation for heterogeneous ip-based mobile ad-hoc networks.

2. LITERATURE REVIEW

Capra and Musolesi [1] have proposed a pervasive trust model inspired by human system. In that work they used Kalman filter theory to predict the future state of the system. New trust observations are fed in by means of a set of recursive mathematical equations to increase the accuracy of the prediction. It calculates the discrepancy between the trust value claimed by the node and the actual trust value. Based on this discrepancy the trust of the node will be predicted.

Another reputation prediction model based on Kalman filter is proposed by Wang et al. [2]. The reputation values received from different nodes are aggregated in the feedback system in Kalman filter. Kalman filter also produces the prediction variance. This variance is used to predict the reputation of the target node.

A trust prediction algorithm based on the concepts of trust mirroring and trust teleportation is proposed by Skopit et al. [3]. In trust mirroring, the environment, interest and competency similarities of people are interpreted directly as an indicator for future trust.

Ming Yu et al. [4] have proposed a link availability-based QoS-aware (LABQ) routing protocol for mobile ad hoc networks based on mobility prediction and link quality measurement, in addition to energy consumption estimate. Yung Yi and Sanjay Shakkottai [5] have developed a fair hop-by-hop congestion control algorithm with the MAC constraint was being imposed in the form of a channel access time constraint. In the absence of delay, they have shown that this algorithm was globally stable and has the property of spatial spreading.

R.Asokan et al. [6] were being extended the scope to QoS routing procedure, to inform the source about QoS available to any destination in the wireless network. However, existing QoS routing solutions were dealt with only one or two of the QoS parameters. They have proposed a QoS Dynamic Source Routing (DSR) protocol using Ant Colony Optimization (ACO) called Ant DSR (ADSR).

Duc A. Tran and Harish Raghavendra [7] have proposed CRP, a congestion-adaptive routing protocol for MANETs. CRP tried to prevent congestion from occurring in the first place, rather than dealing with it reactively. A key in CRP design was the bypass concept. A bypass was a sub path connecting a node and the next non congested node. If a node was aware of a potential congestion ahead, it was found a bypass that was used in case the congestion actually occurred or. The congestion was avoided as a result.

RamaChandran and Shanmugavel [8] have proposed and studied three cross-layer designs among physical, medium access control and routing (network) layers, using Received Signal Strength (RSS) as cross-layer interaction parameter for energy conservation, unidirectional link rejection and reliable route formation in mobile ad hoc networks.

3. PROPOSED WORK

3.1 Multipath Route Discovery

The proposed work aims in design and development of secured reliable multipath routing protocol (SRMRP) using distributed security scheme and carrier sense multiple access with collision intimation for heterogeneous mobile ad-hoc networks. The following is the methodology of the proposed routing protocol.

Our proposed SRMRP adopts several characteristics as like AOMDV protocol. SRMRP is based on the distance vector concept and uses hop-by-hop routing approach. In addition, SRMRP discovers routes on demand using a route discovery mechanism. In our proposed SRMRP, route request (RREQ) proliferation from the source node towards the destination node that launches multiple reverse paths both at intermediate nodes as well as the destination node. Many route replies (RREPs) pass through the reverse paths back which forms multiple forward paths to the destination at the source and intermediate nodes. It is a noteworthy fact that SRMRP offers intermediate nodes with alternate paths as they are found to be useful in reducing route discovery frequency. The nucleus of the proposed SRMRP exists in make certain that multiple paths discovered are loop-free and disjoint, and in efficiently finding such paths using a flood-based route discovery. SRMRP route update rules which are similar to AOMDV [9], applied locally at each node, play a key role in maintaining loop-freedom and disjointness properties. As in the conventional Unipath routing protocol AOMDV, when a traffic source needs a route to a destination, the source node initiates a route discovery mechanism by generating a RREQ. As the RREQ packets are flooded network-wide, a mobile node may receive several copies of the same RREQ. Therefore, all duplicate copies are examined in SRMRP for possible alternate reverse paths, but reverse paths are formed only using those copies that preserve loop-freedom and disjointness among the resulting set of paths to the source node. Whilst an intermediate node obtains a reverse path via a RREQ copy, it checks whether there are one or more valid forward paths to the destination node. If so, the node generates a RREP and sends it back to the source along the reverse path; the RREP includes a forward path that was not used in any previous RREPs for this route discovery. In this case, the intermediate node does not propagate the RREQ further. If not, the node re-broadcasts the RREQ copy if it has not previously forwarded any other copy of this RREQ and this copy resulted in the formation/updation of a reverse path.

3.2 Sorting the Routing Table

After the routes are discovered, this step performs a very important step by sorting the discovered routes based on number of hops. This step is performed to identify which route(s) is/ are having less number of hops so that shortest available route is found.

3.3 Trust Estimation on Discovered Routes and Removal of Un-Trusted Routes

In this section a trust computation scheme which is based on direct observations to establish trust among mobile nodes is presented. After sorting the routing table each mobile node measures the trust of the other nodes by analyzing their behavior over time in the route. For example, node A observes the behavior of node B and adjudicates whether the behavior is correct or not. Each opportunity of mobile node A has of observing the behavior of mobile node B is being recorded in an experience record cache. After some time, these experiences will become obsolete. Therefore, node A will assign some weight values which will be decreasing function with time to the past record. At this point, trust is represented as mean trust value and a confidence interval about the mean. It is assumed that Ai is the inference by node A on node B's behavior at time i and the weight factor assigned to this inference is Wi. The mean value of implication over time n is formulated and given below as

$$\overline{A}=\sum_{i}^{n}\left(\frac{W_i}{\sum_{i}^{n}W_i}A_i\right) \quad (1)$$

The value Wi depends on both the behavior of node B at ith experience and also the trust value of node A in measuring the trust of node B. Here the variance around the mean is formulated and given below implication over time n is formulated as

$$\sigma^2=\sum\left(\frac{\sum_i\left(A_i-\overline{A}\right)^2}{n-1}\right) \quad (2)$$

Now the weight variance is given by

$$\sigma_A^2 = \frac{\sigma^2 \sum W_i^2}{\left(\sum W_i\right)^2} \quad (3)$$

The weighted variance is used to create a confidence interval about the mean as follows

$$x \pm t_{n-1}, 1-\alpha/2\sqrt{\sigma_w^2/n} \quad (4)$$

Where is 0.10 for 90 % confidence interval, 0.05 for 95 % confidence interval and so on. The t indicates the distribution. If the confidence interval is sufficiently narrow then node A will proceed with the decision making process. However, if the confidence interval is too wide then additional experiences will be collected.

3.4 Packet Transmission and CSMA/CI

Collision occurs when a nearby transmitter mobile node interferes with reception node, causing packet corruption. The way to detect such collisions, receiver node finds for a PHY-layer preamble in its incoming signal. The process searching happens through correlation of the preamble with the signal arriving at receiver node's antenna that happens in parallel fashion and does not affect the normal packet decoding procedure. Once transmitting node's preamble impinges on receiving node's antenna, the correlation exhibits a point, which in turn arise an alert that the packet may be in some trouble. The confidence value is an indicator of how likely a bit is in error. Depending on a window of confidence observations, infers whether the packet is expected to get corrupted. If so, halts reception and prepares to send a collision notification to transmitter node. Now, if the interferer starts first, and the transmission from starts later, may need to abort. Though, must first ensure that the later-arriving signal is actually meant for itself. Foreword correlation is not sufficient because may use the same preamble for transmitting to some other receiver; should not send an abort then. To sum up, the receiver node searches for a preamble while receiving its frame of interest, but searches for its own signature while receiving an interfering frame. Upon detecting a collision, stops receiving and prepares to transmit collision intimation (CI). The CI is composed of only receiving node's own signature. Any signature mechanism can be passed. Here the conventional RSA data security digital signature is used. The receiver node transmits the CI packet like a regular 802.11 ACK—there is no carrier sensing, hence the CI is transmitted even though the transmitter is still transmitting. The listening antenna of the transmitter node continuously correlates for the receiver's signature in the incoming signal. This correlation is more challenging because the self-signal is much stronger than the intimation. It is shown that even then the listener node can distinguish the intimation with steady accuracy. Ahead detecting the collision intimation, the listener node immediately alerts the transmitting interface, which then suspends the transmission. The appropriately aborted transmitter backs off as prescribed in IEEE 802.11 MAC. Other mobile node in the glance takes up this opportunity to transmit. Suppose no other mobile node transmits, the same transmitter may resume the transmission of the aborted frame.

In CSMA/CI, the transmitter node does not retransmit the entire aborted packet. As an alternative, it resumes transmission from byte REC_BYTE, where REC_BYTE indicates the maximum in-sequence byte received correctly by the receiver. REC_BYTE can be estimated because the receiver node takes a stable time to identify the collision after its occurrence, responds with a fixed-size collision intimation which occurs after Short Inter Frame Space (SIFS) interval, and the transmitter node detects the intimation signature in a stable time. In case when the transmitter node receives intimation while transmitting byte TR_BYTE where, the estimate of bytes REC_BYTE = TR_BYTE – OUT_BYTE, is resolved based on the transmission bit rate. For example, in our design, collision detection takes time equivalent to 20 B. The time for intimation signature of 10 B over 10-MHz bandwidth is 4 s. Therefore, the turnaround time for intimation including the SIFS interval of 5 s would be 9 s. This matches to 61 B at 27 Mb/s which includes the collision intimation overhead of 10 B, a conformist estimate of 75 B. Therefore, when a sender node is transmitting a 750-B packet and aborts transmission at the 374th byte, it will recommence from the 300th byte. Once the packet is transmitted, the CSMA/CI receiver node responds with an ACK when it is received correctly. Though, unlike 802.11 ACK frame, CSMA/CI ACK is simply a digital signature. When no ACK signature returns from the receiver node, the transmitter node times out and retransmit the entire packet. It is proved from the extensive simulation results that the proposed CSMA/CI mechanism is a simpler approach to 802.11 MAC. The following two pseudocodes project the core flow of operations under CSMA/CI.

```
Algorithm 1: Transmitting (TR)
Start sending frame Preamble: Sign(R): Data
Keep listening and correlating with Sign(R)
If Corr (Sign(R)) high then
        Suspend and resume TR after backoff
If no Corr (Sign (ACK(R))) at the end of TR then
        Retransmit after a random backoff

Algorithm 2: Receiving (REC)
If frame of interest is already being REC then
        If Corr (Pre) high and many bits suspect then
                TR Sign(R)
If interfering frame is being REC then
        If Corr (Sign(R)) high then
                TR Sign(R)
If frame of interest rec successful then
        TR Sign (ACK(R))
```

3.5 Advantages of SRMRP

1. The proposed SRMRP is secured since the existing Ad hoc On-demand Multipath Distance Vector (AOMDV) routing protocol is not concerned about trust.

2. This scheme concerns much about packet transmission & errors and hence reliable data transmission is ensured.

4. SIMULATION SETTINGS AND PERFORMANCE METRICS

4.1 Simulation Settings

Network Simulator 2 (NS2) is used to simulate SRMRP and AOMDV protocol; 100 mobile nodes starting from IP address 192.168.1.1 to 192.168.1.100 move in a 1500 x 1500 meter rectangular region for 100 seconds simulation time. The channel capacity of mobile nodes is set to the value ranging between 0.5 to 2 Mbps. We use the distributed coordination function (DCF) of IEEE 802.11 for wireless LANs. It has the functionality to notify the network layer about link breakage. We assume each node moves independently with the different mobility speed between 0.5 m/s to 3 m/s. All nodes have the different transmission range ranging between 100 to 250 meters. The simulated traffic is Variable Bit Rate (VBR) with varying initial energy between 1.75 to 2.5 joules. 10 nodes are configured as malicious nodes and injected into the simulation. Since the real-time ad hoc networks are heterogeneous, in this simulation the optimum level of heterogeneity in configuring the mobile nodes is done. The simulation settings are also represented in tabular format as shown in Table 1.

Table 1. Simulation Settings

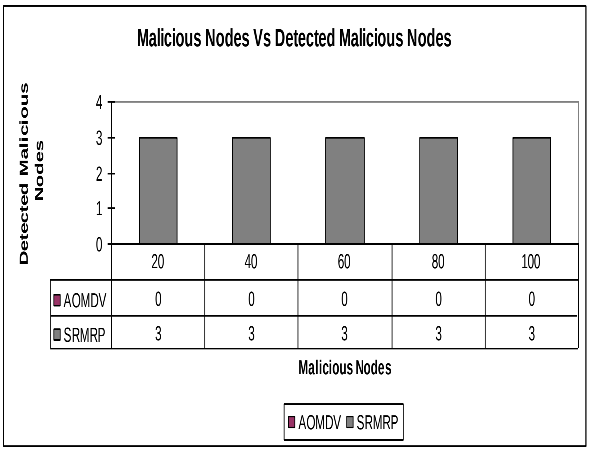
No. of Nodes	100
Terrain Size	1500 X 1500 m
MAC	802.11b
Radio Transmission Range	100 to 250 meters
Simulation Time	100 seconds
Traffic Source	VBR (Variable Bit Rate)
Packet Size	512 KB
Mobility Model	Random Waypoint Model
Speed	0.5 m/s to 3 m/s

4.2 Performance Metrics

The metrics are taken into account for comparing performance of the proposed SRMRP and AOMDV routing protocol. The metrics for both security and Reliability is extensively simulated using NS2. For security, the number(s) of detected malicious nodes and normalized control bytes metrics are taken. For ensuring reliability, the metrics such as packet delivery ratio and throughput metrics are taken.

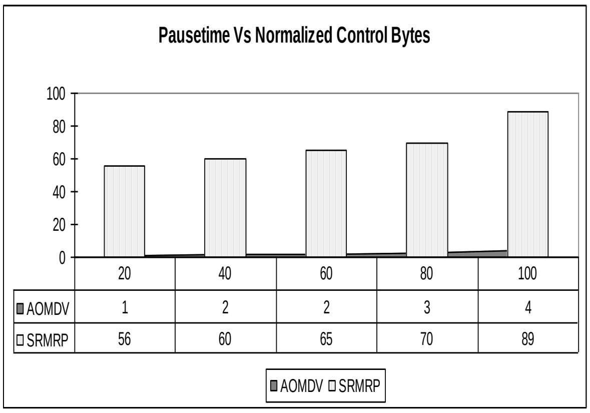
5. RESULTS AND DISCUSSIONS

In Fig.1 the performance the number(s) of detected malicious nodes is compared with conventional AOMDV routing protocol with the proposed SRMRP. From the extensive simulation results obtained from NS2 it is observed that the proposed SRMRP detects all the injected malicious nodes. It can also be observed that AOMDV does not detect any of the injected malicious nodes in the simulation environment since AOMDV does not have any security mechanisms. From Fig. 2, normalized control bytes metric it can see that the proposed SRMRP has reduced normalized control bytes. Fig.3 shows that the throughput is more in SRMRP compared to AOMDV. In Fig. 4, it can be see that, delivery ratio is higher than that of AOMDV routing protocol.



	20	40	60	80	100
AOMDV	0	0	0	0	0
SRMRP	3	3	3	3	3

Fig. 1. Injected Malicious Nodes Vs Detected Malicious Nodes



	20	40	60	80	100
AOMDV	1	2	2	3	4
SRMRP	56	60	65	70	89

Fig. 2. Pausetime Vs Normalized Control Bytes

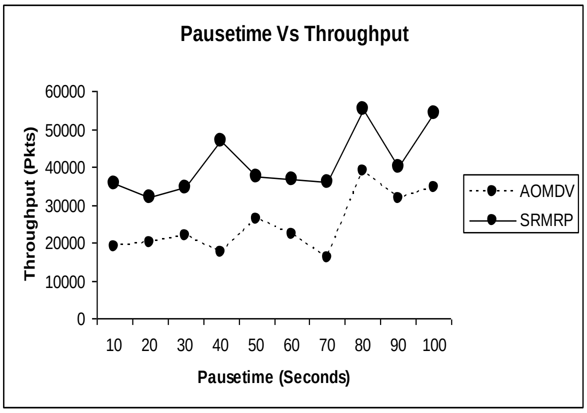


Fig. 3. Pausetime Vs Throughput

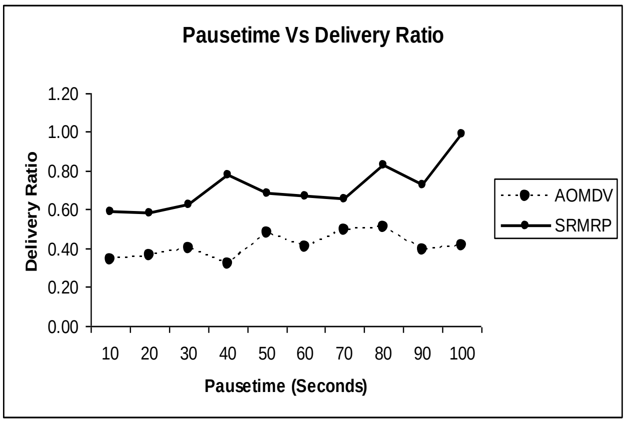


Fig. 4. Pausetime Vs Delivery Ratio

6. CONCLUSIONS

This research paper proposed Secured Reliable Multipath Routing Protocol (SRMRP) using Trust Computation and Carrier Sense Multiple Access with Collision Intimation for Heterogeneous IP-based Mobile Ad-hoc Networks which aims at two main objectives. The first objective is to make the communication secured against attacks. For achieving this reference based trust security mechanism is proposed. The next objective is to provide reliable data communication in heterogeneous mobile ad hoc network. For achieving this adaptive carrier sense multiple access with collision intimation mechanism is employed. The simulations are done in NS2. The simulated mobile nodes with different capabilities such as transmission range, channel capacity and initial energy are configured. Extensive simulation results prove that our proposed SRMRP achieves better reliability in terms of increased throughput and packet delivery ratio. The security performance metrics such as the number(s) of detected malicious nodes and normalized control bytes are taken and SRMRP achieves better results when compared to existing AOMDV routing protocol.

7. ACKNOWLEDGEMENTS

The first author thanks the management of Dr.N.G.P. Educational Institutions for providing career opportunity as an Assistant Professor in the Department of Computer Technology at Dr. N.G,P. Arts and Science College, Coimbatore. The second author thanks UGC for allocating Minor Research Project grant during Feb 2011 to Feb 2013 Grant Number 39-947/2010 (SR).

8. REFERENCES

[1] Capra, L., Musolesi, L.: Automatic trust prediction for pervasive systems. Proc. 20th International Conference on Advanced Information Networking and Applications. (2006) 481-488

[2] Wang, X., Liu, L., Su, J..: Rlm: A general model for trust representation and aggregation. IEEE Trans. Services Comput. 99 (2010) 231-243.

[3] Skopik, F., Schall, D., Dustdar, S.: Start trusting strangers? Bootstrapping and prediction of trust. 10th International Conference on Web Information Systems Engineering. (2009) 112-118.

[4] Ming Yu., Aniket Malvankar., Wei Su., Simon Foo.: A link availability-based QoS-aware routing protocol for mobile ad hoc sensor networks. Computer communications Archive.3018 (2007) 3823-3831.

[5] Yung Yi., Sanjay Shakkottai.: Hop-by-Hop Congestion Control Over a Wireless Multi-Hop Network. IEEE/ACM Transactions on Networking.151 (2007) 2426-2439.

[6] Asokan. R., Natarajan. A. M., Venkatesh. C.: Ant Based Dynamic Source Routing Protocol to Support Multiple Quality of Service (QoS) Metrics in Mobile Ad Hoc Networks. International Journal of Computer Science and Security. 23 (2008) 48-56.

[7] Duc Tran., Harish Ragavendra.: Congestion Adaptive Routing in Mobile Ad Hoc Networks. IEEE Transactions on Parallel and Distributed Systems. 1711 (2006) 1262-1274.

[8] Ramachandran., Shanmugavel.: Received Signal Strength-based Cross-layer Designs for Mobile Ad Hoc Networks. IETE Technical Review. 254 (2008) 192-200.

[9] Mahesh K. Marina, Samir R. Das.: Ad hoc on-demand multipath distance vector routing. ACM SIGMOBILE Mobile Computing and Communications Review. 63(2002) 92-93.