

A Hybrid Trust Model for Mobile Ad Hoc Networks

R.L. Gordon and D.S. Dawoud

School of Electrical, Electronic and Computer Engineering

University of KwaZulu Natal, King George V Avenue, Durban, South Africa, 4041

Tel: +27 31 2602751, Fax: +27 31 2111

email: GordonR@ukzn.ac.za; dawoudd@ukzn.ac.za

Abstract—Trust establishment is a key aspect of network management. Establishing trust in a wireless ad hoc network environment is a challenge because of its unique characteristics. These include the lack of a central authority and the autonomous, dynamic nature of these networks which result in poor connectivity and routing failure. Security may be provided through conduct analysis and certificate based techniques, such as digital certificates. We propose a hybrid trust model for mobile ad hoc networks, combining certificate and conduct based trust to provide secure communication. The security scheme occurs in an on-demand, fully distributive, wireless ad hoc network environment, establishing trust on the routing layer exclusively. Simulations show the overhead of the proposed scheme and that it has negligible impact on network performance while providing trust establishment for the network.

Index Terms—Wireless ad hoc network security, trust establishment, key distribution, conduct trust

I. INTRODUCTION

Wireless ad hoc networks are complex networks which have little or no existing network infrastructure. This lack of fixed network architecture creates complex security problems. The term secure trust is defined as the “belief by a trustor with respects to the competence, honesty, security and dependability of a trustee within a specific context.”[1]. There are two main approaches for trust establishment: certificate based trust models [2, 3] and conduct based trust models [4, 5].

Certificate based trust models use vital keying material to provide trust. There are two trust variables: direct trust and indirect trust. Direct trust is a result of independent or local trust evaluation, between two immediate nodes. Indirect trust is evaluated using the advice from other nodes. In the context of certificate based trust direct trust is defined as trust between local neighbours and indirect trust is created by certificate chaining. Key management is central to certificate based trust establishment [2, 3, 6]. One primary task of key management is the distribution of the keying material for example self-certificates. In a fixed network an on-line trusted authority is present to perform key management tasks. This is not possible in an ad hoc network which lacks a central trusted authority or fixed network infrastructure. Literature shows that there are two main approaches to solve this problem. A partial distributive scheme [3, 7] which distributes the

functionality of the trusted network authority amongst a limited number of nodes. The second approach is a fully distributive scheme [2, 8] which distributing the security responsibilities across the entire network. In a fully distributive scheme each node is considered to be the centre of its own world, and is responsible for its own secure communication [2].

Achieving key management and more specifically key distribution in mobile ad hoc networks is a challenge due to the lack of a central authority and the autonomous, dynamic nature of these networks which result in poor connectivity and routing failure. Many secure routing protocols for mobile ad hoc networks are published, e.g. SAODV [9], and endairA [10]. Most of these neglect the task of key distribution, assuming pre-existing and pre-sharing keying relationships. Key management proposed in [7-9, 11] operates on the routing layer to achieve key distribution. The routing request packets are enlarged by appending the required certificates to all routing requests in an effort to distribute keying material. This approach is not ideal for an on-demand ad hoc network environment because it results in flooding the network with enlarged routing request packets during its route discovery phase.

Secure protocols exist that provide key distribution [6, 11, 12] but these schemes lack to consider the delay incurred from the key management task of verification, assuming it to be negligible. Existing models have such delayed bootstrapping security phases that security is only delivered after an initial time of setup. This creates a window period of weakened security or restricted communication [4, 6].

Conduct based trust models are reactive models which use nodal behaviour to establish trust. Providing conduct based trust enhances the trust decision made by nodes affecting keying decisions. Evidence is gathered by monitoring neighbouring nodes, providing direct trust. Indirect trust is evaluated using recommendations from other nodes. The evaluation of indirect trust has several methods of different complexity from weighted trust average [13], to probabilistic distributions [14] and the semiring mathematical approach [5] which provides special mathematical operators to aggregate trust. By combining certificate and conduct based frameworks this allows for the benefits of the robust certificate model to be combined with the conduct based model which adds integrity to trust by including trust evidence based on nodal behaviour

The aim of our paper is to design a security scheme that can establish trust in a wireless on-demand ad hoc network, with negligible effects upon routing performance. The security scheme establishes trust through a hybrid

certificate, conduct trust model. Providing the key management tasks of key distribution and verification and complimenting this certificate based trust with a conduct based trust model. The scheme has the following constraints:

- The scheme is to operate in a fully distributive, on-demand environment, exclusively on the routing layer.
- The trust mechanism aims to minimize the security overheads which affect the network routing performance. These overheads include trust evaluation, certificate verification and distribution delays.
- The security scheme should allow conduct of nodes to influence the trust decision.
- The trust mechanism should avoid altering the routing mechanism, and strive for independence between routing and trust establishment. Routing packet size is not to be extended to incorporate security information.
- There should be no existence of an on-line trust authority or prior trust relationships.
- Security should be available as a node enters a network with a seemingly insignificant bootstrapping phase.
- This scheme should be robust to poor connectivity and routing failure due to shifting mobility, error-prone wireless channels and traffic congestion which are natural characteristics of wireless ad hoc networks.

The proposed scheme is called Direct, Indirect Trust Distribution (DITD) and it follows the procedure outlined in Section II. The paper is structured in the following manner: In Section II the Direct, Indirect Distribution scheme is proposed, describing the certificate and conduct based trust mechanisms. Section III includes the implementation, simulation and evaluation of DITD's performance. Section IV provides closing conclusions.

II. PROPOSED SCHEME

A. System Model

To fulfill the constraints given in Section I, we assume the following system model. There is no pre-existing infrastructure and no online trusted third party present during communication. The model is a fully distributive network of wireless nodes using an ad hoc on-demand routing mechanism. It is assumed that nodes have their own keying material before joining the network generated by a fully self organized mobile ad hoc network [2], or by an off-line authority issuing keying material before a node enters the network for example in [6]. Each node is assumed to have a public and private key pair, a certificate binding the public key and user identification of the node, and a set of network security parameters common to all nodes in the network. The DITD model uses conduct trust evaluation and the assumption is made that conduct trust evidence is available and that each node has been assigned an individual trust value like in [15, 16]. Secure communication is requested from the start to the end of the network lifetime, unlike [4, 6] which is flawed by its initial setup phase with weak security.

B. Proposed DITD Model

The proposed Direct, Indirect Trust Distribution Model

(DITD) aims to provide security by uniting certificate and conduct based trust establishment on the routing layer. DITD is a trust model itself that uses an existing mobile ad hoc routing for implementation. It is not specific for a single routing protocol but its principals can be applied to any routing scheme. In the following we introduce the proposed scheme in AODV environment.

AODV [17] routing procedure has three stages: 1) *sending the request message*; 2) *receiving the request message*; and 3) *sending the reply message*. In the first stage, the originator node A requests communication with destination node B by broadcasting a routing request $RREQ$ into the network. This request is forwarded by intermediate nodes and propagated through the network to B . When the $RREQ$ message is received by an intermediate node P , it may have been sent by A or forwarded by a neighbouring node NP . Upon receiving the $RREQ$ message stage two begins. At stage two a reverse route to A is then set up and P checks if it is the destination B or has a fresh route to the destination node B . If not, then the $RREQ$ is further broadcast by P and propagates until the destination is found. When the destination or a fresh route to the destination is found, stage three commences. A reply message $RREP$ is propagated along the reverse route until it reaches the originator node A establishing the communication route.

DITD is divided into conduct based trust and certificate based trust establishment and both subdivisions are explain with reference to the AODV routing procedure.

1) Certificate based trust

When a node receives a routing control packet, DITD sends certificate requests using separate unicast messages. The self certificate distribution is added at stage two and stage three; the receiving of the route request and the sending of the reply message stages. At stage two, upon receiving a route request packet, before this packet is processed and the routing table updated, direct trust and indirect trust establishment is set up. The certificate based proposal is further divided into three parts: Direct trust establishment, indirect trust establishment and the post verification optimization.

a) Direct Trust

At stage two, when node P receives a route request $RREQ$, it first checks its certificate repository for the certificate of the neighbour, NP , who forwarded the request. If it does not find the certificate, $Cert_{NP}$, a local self certificate exchange is done between node P and its neighbour NP using two unicast messages. The establishment of direct trust follows the $RREQ$ through the network as seen in Fig. 1. What can be expected is an increased packet overhead during route establishment phase.

b) Indirect Trust

At stage two, when node P receives a $RREQ$ it searches for the originator's certificate, $Cert_A$. If it is not found, node P sends a unicast certificate request for $Cert_A$ to NP . This allows for $Cert_A$ to be distributed as it finds the destination B . For indirect certificate trust to be established

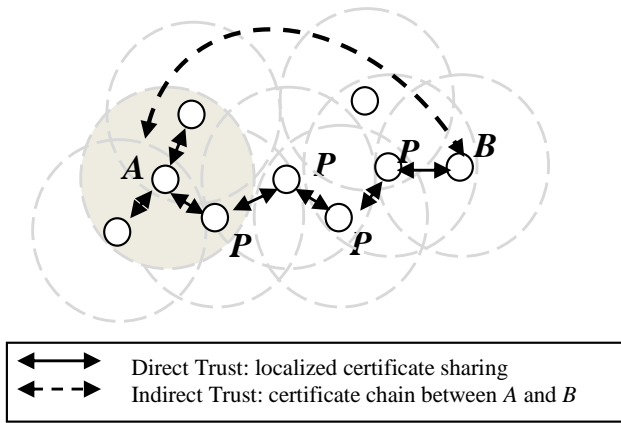


Fig-1 Direct and Indirect trust establishment

originator A is required to possess the destination's certificate, $Cert_B$, as well. At stage three, sending the reply message, the indirect trust establishment is completed by distributing $Cert_B$ with the $RREP$ message. Sending a reply is guided by two conditions. Firstly when the destination node is found and secondly when a fresh route to the destination node is found. For the first condition, the reverse route to A is already setup with localized direct trust existing between nodes on the route; therefore a trusted certificate chain of nodes is available towards the originator node A . It is required only that the certificate of the destination node, $Cert_B$, be piggy backed on the routing reply message $RREP$ toward B . Each intermediate node stores $Cert_B$ and updates its certificate repository. For the second condition, if a fresh route to B is found, there exists a route from intermediate node P to destination B and a route from P to A . Both routes have existing localized direct trust, so the two routes can be view as certificate chains. Two $RREP$ messages are then propagated, one toward B with $Cert_A$ appended and one toward A with $Cert_B$ appended. Indirect trust is therefore set up by certificate chaining as illustrated in Fig. 1.

c) Verification

Verification upon an indirect trust chain requires each node to verify its chain neighbour, the originator and destination node's certificate. Ideally verification will take place immediately after a certificate is received but the processing of a single verification results in a computational delay. For application specific networks that are time dependent like military automation networks a delay of even milliseconds is critical. DITD provides optimized verification by allowing routing messages to be forwarded pending verification confirmation.

Verification for direct trust establishment can be done immediately without incurring a delay upon the routing mechanism. This is because the localised certificate messages are separate and independent from the request messages. Furthermore during route discovery, $RREQ$ messages can be forwarded without waiting for verification to be processed [8] as verification can be confirmed on the reply route. Such delayed confirmation of verification is not possible for the $RREP$ message and certificates must be verified before the $RREP$ message can be securely forwarded and trusted routes established. Therefore the problem is that the verification of the destination certificate

$Cert_B$ may cause a delay in route establishment because $Cert_B$ is distributed with the $RREP$ message.

A solution to this is the use of back tracked verification. If any intermediate node has $Cert_B$, it can distribute $Cert_B$ to the reverse route, during $RREQ$ message propagation. This is achieved by adding a flag, $flag_{cert}$, to each route entry indicating if the previous hop as or does not have the destination certificate. When a $RREQ$ message is forwarded a flag is appended identifying if the forwarder has the destination certificate $Cert_B$. When Node P receives a $RREQ$ it checks if it has $Cert_B$. If it has $Cert_B$ and the reverse route variable $flag_{cert}$ indicates that the previous hop does not have $Cert_B$ then P sends a unicast certificate message containing $Cert_B$. The $Cert_B$ is propagated along the reverse route by checking the routing table entry $flag_{cert}$ and responding in a respectively. This allows the destination certificate $Cert_B$ to be distributed during route discovery phase independent from route establishment.

The verification is completed with minimal delay incurred upon the route establishment. The neighbour and the originator certificate ($Cert_A$) are verified without causing any delay upon the route discovery. The destination certificate ($Cert_B$) is verified with the $RREP$ message, and this delay is alleviated by a prior distribution of $Cert_B$ on the reverse route where it is possible.

Direct and indirect trust establishment is realised through the route establishment phase of the ad hoc routing scheme. During the initial stage of route establishment the network is flooded with routing requests and in turn certificate exchange messages. It can be expected that there will be a large packet overhead during the initial trust establishment stage.

2) Conduct based trust

The DITD model proposes methods to allow for conduct trust evaluation on the routing layer. Ideas from the modified proactive generic-single-source-shortest-distance algorithm [5, 18] are inherited and we propose to apply this semiring mathematical formulae more specifically to the reactive on-demand route discovery phase of the routing protocol.

Trust values are assumed to be made available and the DITD scheme focuses upon the evaluation of the trust values by aggregating them along a path. During route discovery trust is aggregated along the $RREQ$ path using the semiring mathematic operator \otimes [18]. The trust is aggregated along a path like parallel resistors would be

summed i.e. $\frac{1}{T_r} = \frac{1}{T_1} + \frac{1}{T_2} + \dots + \frac{1}{T_n}$. The trust

decreases along the path and the final trust can be no larger than the lowest trust value. This aligns with the description of a trust chain which states a chain is only as strong as its weakest link. DITD model further requires that each node participating in the route discovery phase has a certain minimum trust level. This effectively filters out any certificate trust paths lower than a threshold trust of $trust_{thresh}$. If a trust chain is as strong as its weakest link, the DITD model makes sure that its weakest link is of a suitable trust level $trust_{thresh}$. The AODV approach selects the shortest path, based upon the number of hops, while the

DITD model selects the most trust path based on an aggregated trust value.

Trust is aggregated along the *RREQ* path and again along the *RREP* path updating the routing table based upon the most trusted paths found. Nodes are only processed if they meet a specified trust threshold.

III. DISCUSSION

A. Performance Evaluation

The DITD model was implemented in C++ as a network layer application for *ns-2* (release 2.31) [19]. A simulation study was made to identify the protocols effects upon the network layer and network performance.

B. Simulation Model

A wireless ad hoc network is simulated using the *ns-2* designed IEEE 802.11b physical layer and medium access control (MAC) protocols. The transmission range of each node was set to 250m. The network area is 1000m x 1000m. The *ns-2* constant bit-rate (CBR) traffic generator was used to simulate the traffic load. The CBR packet size was set to 512 bytes. All the traffic sources are started before the initial 150 seconds, forcing maximum certificate distribution at the network establishment phase. The simulation time is 1500 seconds. The simulation uses the *setdest* mobility model keeping with existing literature using *ns-2*. Mobility was varied at three intervals 0.2m/sec, 5m/sec and 20m/sec simulating a network with low, moderate and rapid mobility.

The OpenSSL library is used for certificate verification analysis. The size of the certificates was set to 450 bytes and ECC (Elliptic Curve Cryptography) is used simulating a 160ms verification time on a Compaq iPAQ 3670 according to [8]. The Ad Hoc On-demand Distance Vector (AODV) routing protocol [17] is used. The DITD model is implemented by modifying the AODV protocol in C++ providing the security model as a network layer application.

C. Simulation Results

1) Certificate Distribution

Network performance can be analysed by the following metrics: packet delivery ratio (PDR) and end-to-end packet delay. The success rate of communication is represented by the PDR factor and the speed of the communication is represented by the end-to-end delay. We compare the proposed DITD to a reference routing protocol AODV to investigate performance correlation between the two under differing load, node density, and mobility conditions.

In Fig. 2(a) and Fig. 2(b) it is observed that DITD has a strong correlation to the AODV reference simulation for PDR across varied load, mobility and number of nodes. Fig. 3(a) and Fig.3(b) show that the DITD model adds no significant delay for a varying load, mobility and number of nodes. The observation is made from these four graphs that the DITD model has negligible impact on the network performance for an increasing number of nodes and a varied traffic load.. Furthermore the DITD model is observed to have negligible impact on network performance for 0.2 m/sec, 5 m/sec, 10 m/sec, and 20 m/sec mobility. Mobility is exploited in DITD and it is observed in Fig2. (a) that as the mobility increases the correlation between the

simulation models not only become stronger but DITD begins to outperform the AODV reference model, simulating a greater PDR at higher motilities. Capkun [6] proposes a security model which relies on mobility to distribute certificates in a more efficient manner, thus creating a security dependency upon mobility. In Fig-2(a) at 0.2 m/sec, representing an almost stationary network, the reference AODV and proposed DITD simulations maintain strong correlation. This shows that DITD is not dependent on mobility, therefore breaking the dependency relationship between security and mobility but maintaining the benefits gained by increased mobility.

2) Trust Establishment Analysis

The trust establishment phase is identified as the initial 150 seconds of simulation where all traffic commences and routing and security packet overheads are maximised. Fig. 4 shows that during the initial 150 seconds DITD sends an average of 51% more packets than the reference AODV model. These overheads create an unavoidable increase in computation with an expected resultant computational delay. Despite this, Fig. 3(a) and Fig. 3(b) show that the average end-to-end delay has negligible difference to the reference AODV routing protocol. This is because of the fully distributive characteristics of DITD and its independency from the routing mechanism. In [4, 6] two fully distributive certificate exchange schemes are proposed that also experiences excessive overheads at the initial trust establishment phase. Capkun's and Tanabe's approaches rely on initial setup stages to distribute all certificates amongst the network and upon completion of this stage; security would be available to the network. The flaw in this is a resultant window period of weaken security. The DITD model experiences similar packet overheads at the initial stage but allows for secure communication from the start of the network, without weakened security or a significant increase in delay during the bootstrapping phase.

3) Postponed and Back Track Verification

DITD's postponed and back tracked verification alleviates security delays. The simulations analyse the delays caused by ECC (Elliptic Curve Cryptography) verifications with a verification time of 160ms [8]. Four methods are analysed: the *general verification* which verifies certificates immediately after they have been received; *Zapata's method* [8] which uses delayed verification, verifying all the certificates after route establishment; and the *DITD analysis*, simulating DITD with and without back tracked verification. Fig. 5 shows the end-to-end delay of the four verification methods against the AODV protocol. DITD has the smallest delay of only 20ms excess, which is 80% smaller than Zapata's delayed verification method. This is achieved by performing the required verifications independent to route discovery. Fig. 6 shows the number of verifications that affect the delay. DITD minimized the verifications affecting the delay by almost a 1000% compared to the general verification method. To minimizing the delay, DITD relies upon verifications occurring behind the scenes. Fig. 6 shows the total number of verifications and that DITD is more computationally taxing than Zapata's approach. There is a trade off between delay and

computational cost where Zapata's approach provides less computational cost to establish security while DITD provides faster secure route discovery. Therefore the application of DITD would be time dependent networks.

IV. CONCLUSION

In this paper we propose a hybrid security scheme called Direct, Indirect Trust Distribution (DITD). DITD proposes a novel certificate distribution mechanism, a postponed verification mechanism and a conduct trust mechanism to maximise trust establishment. DITD establishes trust by the sharing and verifying self certificates in an on-demand manner on the routing layer. Routing packets are exploited by localized certificate exchanges providing direct trust and indirect trust by certificating chaining. Localising certificate exchange messages, removes trust dependency upon multi-hop routes which are vulnerable to collapse due to the dynamic nature of wireless ad hoc networks. Simulations show that the DITD model does not produce any significant delay or drop in packet delivery ratio for varied load, mobility and number of nodes (Fig. 3 and Fig. 4). This is because of DITD's independency from the routing mechanism and fully distributive nature, allowing secure communication from the start of the network formation. The efficiency of DITD is tested by implementation and trace simulations in *ns-2*. It is concluded that DITD maximizes trust by combining robust certificate trust and conduct trust providing trust establishment through a hybrid trust model for wireless ad hoc networks.

REFERENCES

- [1] T. Grandison, "Trust Management for Internet Applications," Imperial College London, 2003.
- [2] S. Capkun, L. Butty, and J.-P. Hubaux, "Self-Organized Public-Key Management for Mobile Ad Hoc Networks," *IEEE Transactions on Mobile Computing*, vol. 2, pp. 52-64, 2003.
- [3] L. Zhou and Z. J. Haas, "Securing Ad Hoc Networks," *IEEE Network: special issue on network security*, vol. 13, pp. 24-30, 1999.
- [4] M. Tanabe and M. Aida, "Secure communication method in mobile wireless networks," in *MOBILE Wireless MiddleWARE, Operating Systems, and Applications* Innsbruck, Austria: ICST, 2007.
- [5] G. Theodorakopoulos and J. S. Baras, "On Trust Models and Trust Evaluation Metrics for Ad-Hoc Networks," *IEEE Journal on Selected Areas in Communications*, vol. 24, pp. 318-328, 2006 2006.
- [6] S. Capkun, L. Buttyan, and J.-P. Hubaux, "Mobility Helps Peer-to-Peer Security," *IEEE Transactions on Mobile Computing*, vol. 5, pp. 43-51, 2006.
- [7] B. Awerbuch, R. Curtmola, D. Holmer, C. Nita-Rotaru, and H. Rubens, "ODSBR: An on-demand secure Byzantine resilient routing protocol for wireless ad hoc networks," *ACM Trans. Inf. Syst. Secur.*, vol. 10, pp. 1-35, 2008.
- [8] M. G. Zapata, "Key management and delayed verification for ad hoc networks," *J. High Speed Netw.*, vol. 15, pp. 93-109, 2006.
- [9] C. E. Perkins, E. Belding-Royer, and S. R. Das, "Secure Ad Hoc On-demand Distance Vector (SAODV) Routing," 2003.
- [10] G. Acs, L. Buttyan, and I. Vajda, "Provably Secure On-Demand Source Routing in Mobile Ad Hoc Networks," *IEEE Transactions on Mobile Computing*, vol. 5, pp. 1533-1546, 2006.
- [11] V. Balakrishnan and V. Varadharajan, "Designing Secure Wireless Mobile Ad Hoc Networks," in *Proceedings of the 19th International Conference on Advanced Information Networking and Applications - Volume 2*: IEEE Computer Society, 2005.
- [12] J. van der Merwe, D. Dawoud, and S. McDonald, "A Survey on Peer-to-Peer Key Management for Mobile Ad Hoc Networks," *ACM Computing Surveys (CSUR)*, 2006.
- [13] M. Virendra, M. Jadhwal, M. Chandrasekaran, and S. Upadhyaya, "Quantifying Trust in Mobile Ad-Hoc Networks," in *IEEE International Conference on Integration of Knowledge Intensive Multiagent Systems (KIMAS)* Weltham, MA, USA: , 2005, pp. 65-70.
- [14] S. Ganeriwal and M. B. Srivastava, "Reputation-based framework for high integrity sensor networks," in *Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks* Washington DC, USA: ACM, 2004.
- [15] C.-Y. Tseng, P. Balasubramanyam, C. Ko, R. Limprasittiporn, J. Rowe, and K. Levitt, "A specification-based intrusion detection system for AODV," in *Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks* Fairfax, Virginia: ACM, 2003.
- [16] "A Dynamic Trust Model for Mobile Ad Hoc Networks," in *Proceedings of the 10th IEEE International Workshop on Future Trends of Distributed Computing Systems*: IEEE Computer Society, 2004.
- [17] C. Perkins, E. Belding-Royer, and S. Das, *Ad hoc On-Demand Distance Vector (AODV) Routing*: RFC Editor, 2003.
- [18] M. Mohri, "Semiring frameworks and algorithms for shortest-distance problems," *J. Autom. Lang. Comb.*, vol. 7, pp. 321-350, 2002.
- [19] "The Network Simulator," ver 2.31, Available at <http://isi.edu/nsnam/ns/>, 2007.

R.L. Gordon received the BSc degree in Computer Engineering from the University of KwaZulu Natal, Durban, South Africa, in 2006. Starting his MSc Engineering in 2007, his dissertation is concerned with trust establishment in mobile ad hoc networks.

Prof. D.S. Dawoud has been the Professor of Computer Engineering at University of KwaZulu Natal since 2001. During his academic career, he has supervised 10 PhD and about 35 MSc theses and published over 170 papers in international journals and conferences in the fields of: Computer hardware, Digital Signal Processing, and Network Security.

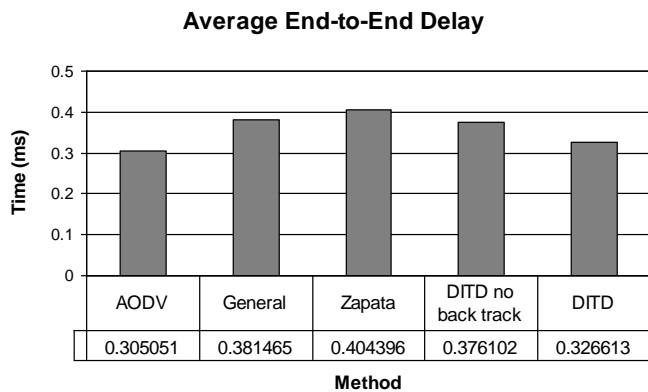
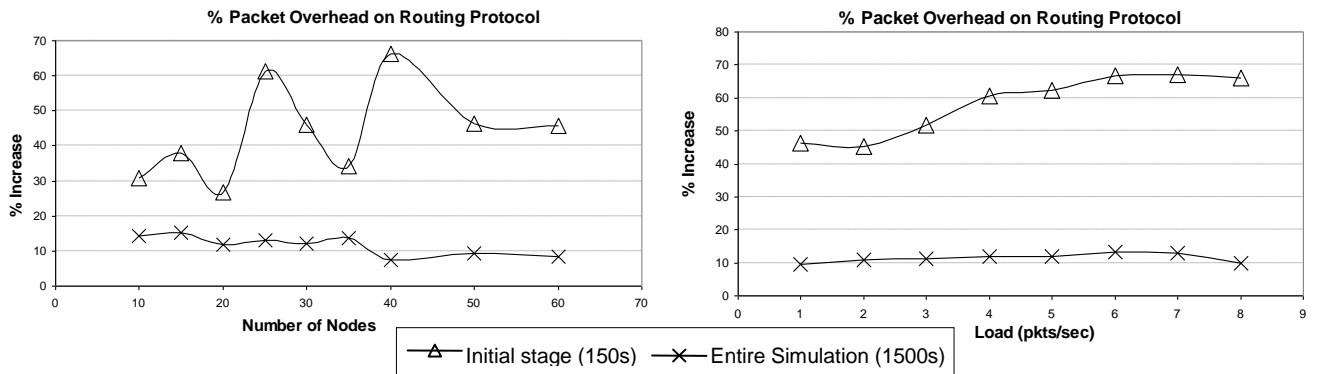
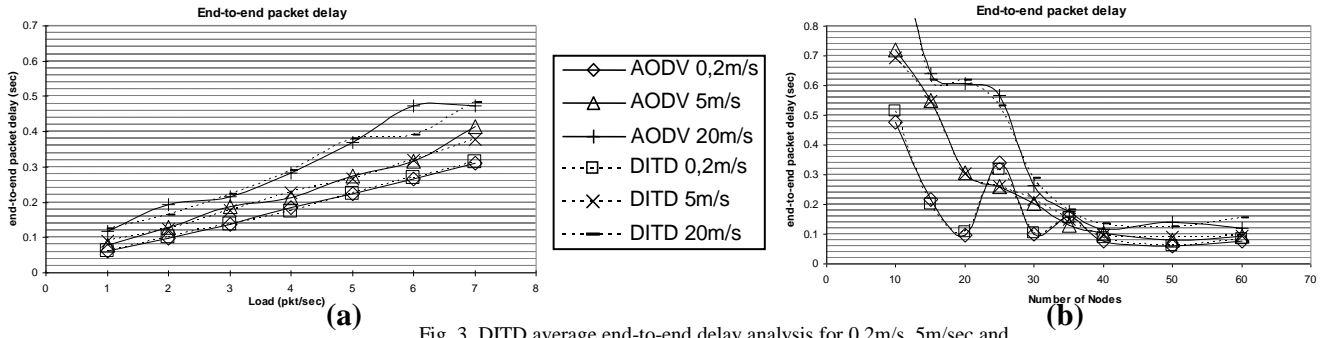
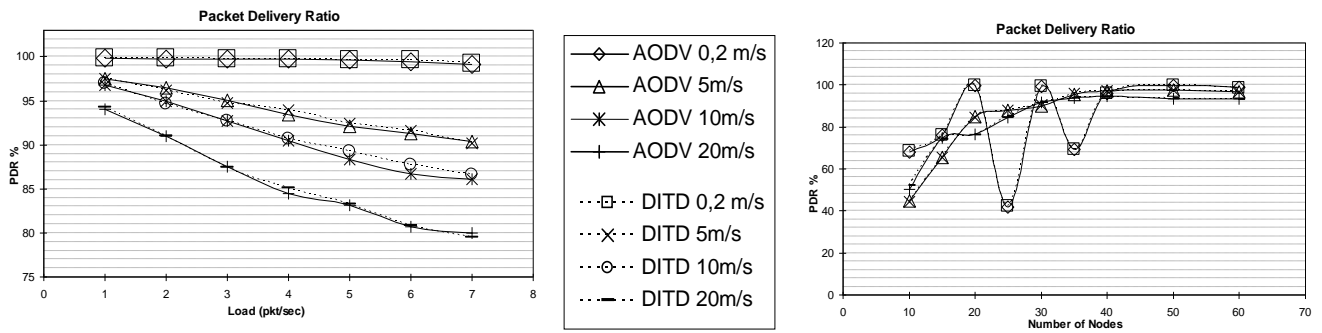


Fig. 5. Average end-to-end delay for 25 node network analysing verification delay

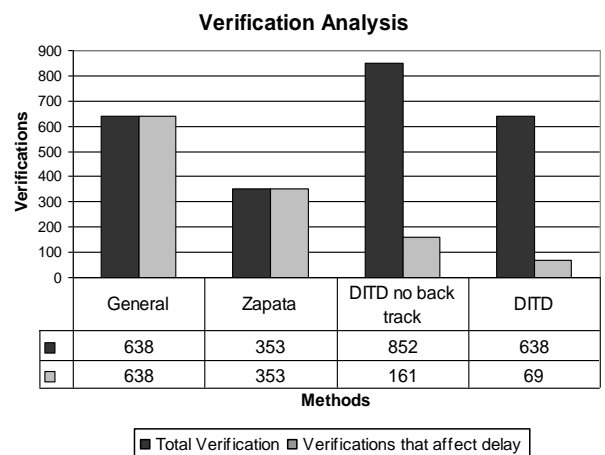


Fig. 6. Verification analysis for 25 node network