Performance and Simulation Study of TheProposed Direct, Indirect Trust Distribution Security Architecture inWireless Sensor Network

[1]Mohammad Reza KaghazGaran, [2]Afsaneh KaghazGaran

[1]kaghazgaran@yahoo.com
[2]af.kaghzagaran@gmail.com

ABSTRACT

In this paper, we propose a routing protocol that is based on securing the routing information from unauthorized users. Even though routing protocols of this category are already proposed, they are not efficient, in the sense that, they use the same kind of encryption algorithms (mostly high level) for every Bit of routing information they pass from one intermediate node to another in the routing path. The proposed mechanism is evaluated against selected alternative trust schemes, with the results showing that our proposal achieves its goals.Our research aims at providing a secure and distributed authentication service in the ad hoc networks.

KEYWORDS

Wireless Sensor Network ; node selection; trust evaluation;

1. Introduction

Mobile host and wireless networking hardware are becoming widely available, and extensive work has been donein the recent years in integrating these elements into traditional networks such as internet.

They can be often used in scenarios in which no infrastructure exists, or in which the existing infrastructure does not meet application requirements for reasons of security or cost. Wireless sensor Network routing protocols are challenging to design and secure ones are even more so. Prior research has generally studied the routing problem in a non-adversarial setting, assuming a trusted environment [3]. These may be sufficient for normal day-to-day applicationsbut for applications such as military exercises and disaster relief, a secure and a more reliable communication is a prerequisite.

Trust-based solutions provide a method to select neighbors based on their trust value which is derived from previous interactions. There have been a number of trust mechanisms proposed for mobile [1],[4] and peer-to-peer networks [5],[7]. Most of these mechanisms are distributed and favors the most trustworthy neighbor.

In this paper, we propose a novel probabilistic node selection model which provides a load balancing within the population of nodes. Hereby, a node's probability for being selected for an interaction will correspond to its trustvalue. Furthermore, it gives unknown nodes the opportunityto be selected, thus enabling these nodes to contribute to the community. trust [5] briefly discusses a similar selection model, but it does not provide an analysis of themodel's

DOI : 10.5121/cseij.2011.1403

impact on the quality of interactions and it allocatesthe lowest possible trust value to unknown nodes.

Achieving key management in mobile Wireless Sensor Network 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 Wireless Sensor Network networks are published, e.g. SAODV [9], SEAD [10], ARIADNE [11], and endairA [12]. Most of these assume pre-existing and pre-sharing keying relationships. Key management proposed in [7-9] operates on the routing layer to achieve key distribution.

The required certificates are appended to all routing request in an effort to distribute keying material during the route establishment phase. This approach is not ideal for an on-demand Wireless Sensor Network in network environment because it results in flooding the network with route request during its route discovery phase.

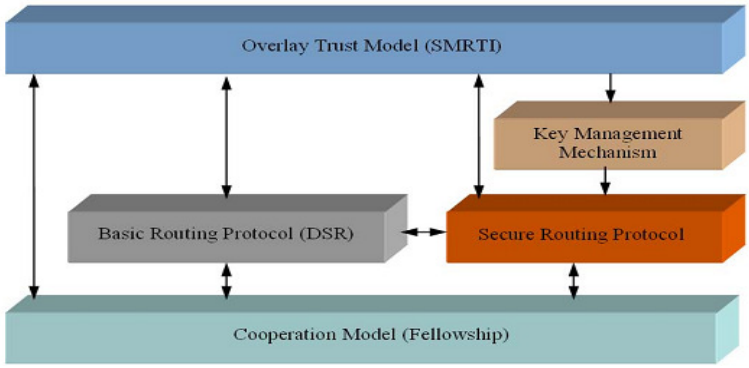

Figure 1: Trust and other security models in Trust Establishment security Architecture for WSN

Secure protocols exist that provide key management tasks such as key distribution [6] 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 weaken security or a window period of restricted communication [4, 6]. The aim of our paper is to design a key management scheme that can be used to distribute and verify certificates in a wireless on-demand Wireless Sensor Networkin network, with negligible affects upon routing performance. The proposed scheme establishes trust by distribute and verify certificates for all the nodes in a network with the following constraints:

- The key management scheme is to operate in an on-demand environment, exclusively on the routing layer.
- The key management scheme is to distribute and verify certificates between local and remote nodes providing direct and indirect trust relationships respectively.
- Each node in an indirect trust chain must verify its neighbor, the originator and destination node's certificates, before the trust chain is secure.
- The key management scheme aims to minimize the security overheads which affect the network routing performance. These overheads include certificate verification and distribution delays.
- The key management scheme 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.

- The certificate scheme is to be designed in a fully distributive manner with 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 timeless bootstrapping phase for security.
- The key management 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 Sensor Network networks.

2. Related work

A detailed survey was presented on key management schemes for mobile ad hoc networks in the previous chapter. Section-2 focused on the network layer and presented a survey of existing secure routing protocols. This section provides work directly related to the DITD model.

The authors of [20],[3] propose a completely self-organized public key system for mobile ad hoc wireless networks. This is a PGP based solution which provides key management in ad hoc networks without the presence of an off-line or on-line authority, like a CA, TTP or server. Each node distributes its self-certificates and maintains its own certificate repositories. Nodes participating in the network share their certificate repositories and repository updates are performed in a proactive manner. Certificates are reciprocally authenticated and trust chains formed linking remote nodes to each other. Security is realized on the application layer.

Zapata [21] addresses the issue of verification delays in secure mobile ad hoc networks. Zapata proposes a protocol to optimize the number of verifications made in a single secure route discovery phase. Once a route is established only then are the shared certificates verified. This helps in reducing the computational overhead of verifications on multi-hop paths. By reducing the total number of verifications made in a network's life time there is a resultant end-to-end delay upon the delivery of routes.

[22] proposes a fully distributive conduct based trust model which has PGP characteristics. This model operates on the application layer and allows for trust to be established without the presence of a central authority member. PGP models share certificates to establish trust while the work proposed in [22] allows for other trust evidence, like conduct and location, to influence the trust establishment. Trust is fully distributed in a proactive manner allowing all nodes to give trust opinions about other nodes.

[23] has more recently been used to model trust calculations in [22]. Trust opinions are mathematically aggregated along a path and trust decisions are mathematically represented. The work in [22] uses Dijsktra's extended algorithm proposed by [24] to include trust. This finds the most trusted path between two remote nodes in a proactive manner.

The majority of literature mentioned function in a proactive manner for application layer solutions. The DITD model is designed on the network layer for a reactive, fully distributive,self-organized, mobile ad hoc network environment. The ideas of some of these protocols have inspired the creation of the DITD model and the impact of these protocols is discussed in Section-6.

3. Proposed Scheme

3.1. 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 anWireless Sensor Network 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 Wireless Sensor Networkin network [2], or by an off-line authority issuing keying material before a node enters the network for example in [6],[8]. 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. 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.

3.2. Proposed DITD Model

The proposed Direct, Indirect Trust Distribution Model (DITD) aims to distribute and verify self-certificates to create direct and indirect trust relationships between nodes. DITD is a certificate based trust model which works with existing mobile Wireless Sensor Network routing schemes. 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 [13],[14] routing procedure has three stages: sending the request message; receiving the request message; and 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 neighboring nodeNP. 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. When a node receives a routing control packet, and before that packet is processed, 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 proposed scheme is subdivided into three parts: Direct trust establishment, indirect trust establishment and the post verification optimization.

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. When a node receives a routing control packet, and before that packet is processed, 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 proposed scheme is subdivided into three parts: Direct trust establishment, indirect trust establishment and the post verification optimization.

3.2.1. Direct Trust

At stage two, direct trust relationships are made by allowing the neighboring nodes to exchange certificates. When intermediate node P receives a route request RREQ it first checks its certificate repository for the certificate of the neighbor, NP, who forwarded the request. If it does not possess such a certificate, Certificate NP, a local self-certificate exchange is done between node P and its neighbor NP using two unicast messages.
The exchange of certificates follows the RREQ. This will flood the network in search of a route to the destination node. Direct trust establishment is illustrated in Figure 2. What can be expected is an increased initial packet overhead.

3.2.2. Indirect Trust

Similar to direct trust establishment, at stage two node P searches for the originator's certificate, Certificate A. If it is not found, node P sends a unicast certificate request for Certificate A to NP whose address can be found at the next hop on the reverse route. This propagates Certificate A to the destination B. For indirect certificate trust to be established originator A is required to possess the destination's certificate, Certificate B, as well. By not appending the certificate to the route requests dependency is reduced between the route establishment and trust establishment. At stage three, sending the reply message, the indirect trust establishment is completed. 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 towardshe originator node A. It is required only that the certificate of the destination node,

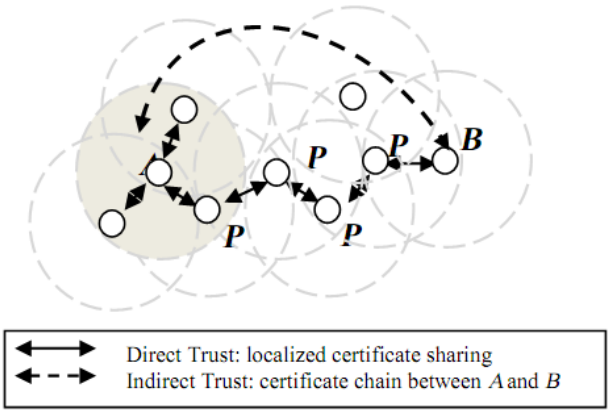

Figure 2: Direct and Indirect trust establishment

Certificate B, to be piggy backed on the routing reply message RREP toward B. Each intermediate node stores Certificate 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 localized direct trust existing already, so the two routes can be view as certificate chains. Two RREP messages are then propagated, one

toward B with the Certificate A appended and one toward A with the Certificate B appended. Indirect trust is therefore set up by certificate chaining as illustrated in Figure 2.

4. Proposed Mechanism

We assume that in Wireless Sensor Network content distribution networks, nodes download the required content from their immediate wireless neighbor's and hence all the communications are single hop. Furthermore, we assume that all neighbors have the required content and that content is sub-divided into several pieces. We propose Real-Time Trust (ReTT), a novel distributed trust evaluation mechanism that continuouslyevaluates trust during an interaction. The mechanism is based on the assumption that an interaction between two nodes will consist of a number of steps which can be individually analyzed in real time.

ReTT introduces two decision points, the decision to connect to a node (decision to start) and the decision to stay connected after the interaction has started (decision to continue).The term real time reflects the notion that newly received information is immediately evaluated to form an evolving evaluation of trust.

The decision to start is determined by a historical trust value of the content-providing node and the context of the interaction. This value is calculated by aggregating the opinions of the selecting node and the recommendationsby other nodes. Let us assume that node d has to make a decision whether to interact with node i. Given that $O_{j,i}$ is the opinion sent to node d by node j on node i, $W_{j,i}$is node d's weighting on $O_{j,i}$, and node d has opinions on i from k nodes (including its own opinion), then the historicaltrust value T_i^H of node d for node i is calculated as follows:

$$T_i^H = \frac{\sum_{j=1}^{k} W_j \times O_{j,i}}{\sum_{j=1}^{k} W_j}$$

$O_{j,i}$ is the average number of good integrity pieces received by node j from node i in a transaction. The decision to start considers a level of openness, which allows the mechanismto

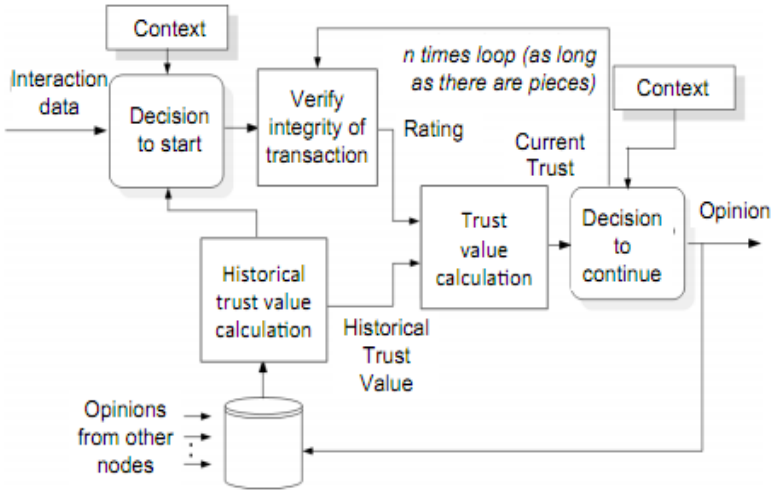

Figure 3: shows an overview of the proposed mechanism.

be flexible depending on the context and introduces a trust level threshold. In a fully open system, this threshold would be the lowest possible trust value, and thus, all availablecontent-providing

nodes are considered as candidates. The remainder of the paper assumes a fully open system.

If the selecting node decides to interact with a content providing node, it then downloads the first piece and evaluates the piece's integrity. In this paper, a piece is considered to have good integrity if it is received as requested and itdoes not contain a virus. The integrity verification result is then combined with historical information to decide whetherto download the next piece (i.e., decision to continue in Figure 3).

Given $T_{i,m}$ is node i's calculated trust value after m_{th} piece in the current interaction, $T_{i,m-1}$ is the trust valueafter receiving the previous and $R_{i,m}$ is the verification result of the current piece, then real-time trust value is calculated as:

$$T_{i,m} = \alpha T_{i,m-1} + \beta R_{i,m} \ , m \epsilon \{1,2,3, \ldots . , n\}$$

and are the weights, with both being positive numbers which sum up to one. Since havingwill ensure that the mechanism quickly responds to changes in behavior.We also propose a novel node selection model which probabilistically selects content providing nodes based on their trust value, which aims to achieve load balancing while still having an appropriate tradeoff for interacting with nodeswith low trust value. To this end, the selecting node evaluates the trust values T of the set of all available content-providing nodes C.

The node probabilistically selects a node from this set C, where the probability of selecting a node n, P_n, is:

$$P_n = \frac{(T_n^H)^{\ x}}{\sum_{i=1}^{|C|}(T_i^H)^{\ x}}$$

We define T_n^H =0,5 only for the selection process, to ensure that unknown nodes are preferred over known misbehaving nodes.

5. TRUST AND REPUTATION

Trust models are an attempt to formalize trust definitions [1] and are often tied to the establishment of a Public Key Infrastructure (PKI) in WSN [75].

In [37], [38], [41] give a security approach based on trust for pervasive computing [42] in which a securityagent (fixed device) in each domain is responsible for trust management, authentication and authorization. A European project, SECURE [28], [66], presents trust and risk frameworks for enabling secure collaboration between ubiquitous computer systems. Establishing trust by physical contact between devices is presented in [67]and extended (to include the use of location-limited channels) in [7].

In addition to this work, the modeling of trust at the network layer has received much attention. Various authors have proposed methods for nodes to establish trust in one another. In this section we provide an overview of these proposals, many of which are designedto tackle the problem of packet forwarding selfishness using preventative and/or reactive measures. The solutions described below can be classed as follows:

- Routing protocol mechanisms,
- Currency systems, and
- Reputation systems.

5.1. Trust in Routing Protocols

This acknowledgementconsists of the packet's unique identifier, concatenated with the destination node's address. If the number of unacknowledged packets exceeds a threshold, then a faultdetection protocol is used, similar to the Secure Trace route protocol proposed by [15]. Thiscontains the addresses of the intermediate nodes from which the originator wants an acknowledgement, with the destination node's address as the last entry. The listincludes a HMAC which is recursively produced, each round using a secret key shared between the originator node and the intermediate node being 'probed' (this is atechnique also known as 'onion encryption' [19]).

When a probed intermediate node receives the probe list, it decrypts a layer of the onion encryption and verifies the HMAC before forwarding the packet, so that the next intermediate node in the probe list can verifythat it belongs to the list.

After forwarding a probe list, an intermediate node waits for an acknowledgement from the next node on the probe list. If one is not received with a specific timeoutinterval, then the node must initiate an acknowledgement chain by creating an acknowledgement. The timeouts arecalculated in such a way that the last probed node which successfully receives the packet will always initiate the acknowledgment chain. Thus, when the route is working,this will be the destination node. This acknowledgement chain is forwarded towards the originator node.

5.2. Reputation Systems

Reputation systems have been proposed for use in Wireless Sensor Network networks to address some of the threats arising from misbehaving network nodes. These mechanisms, explored in more detail in this section, are potentially ofparticular value in addressing the threats arising from selfish nodes. In the context of anWireless Sensor Network, these mechanisms seek to dynamically assess the trust worthiness of neighboring network nodes, with a view to excluding untrustworthy nodes. Although reputationcan be seen as a particular trust metric there have been attempts to draw a distinction between the two.

The use of reputation systems in many different areas of information technology is increasing, not least because of their widely publicized use in online auctions and product reviews.Reputation systems are used to decide who to trust, and to encourage trustworthy behavior. Identify three goals for reputation systems:

1) To provide information to distinguish between a trustworthy principal and an untrustworthy principal,
2) To encourage principals to act in a trustworthy manner
3) To discourage untrustworthy principals from participating in the service which the reputation mechanism is present to protect.

Reputation systems can be managed either centrally or in a distributed manner [36]. As was the case for the discussion of currency systems in section II-B), we concentrate here on distributed reputation systems, which suit the properties of a stub Wireless Sensor Network.

Reputationsystems rely on principals monitoring sequences of transactions with other principals, and on communicationsbetween principals that are willing to take part in the reputation system. Each principal maintains a reputation value for some subset of the other principals in the system. These values can be shared between principals or they may be unique for each participant. The

precisemeaning of the reputation value, how it is calculated and updated, and how it is communicated between parties,are all system-dependent. However, it is generally true that this value is intended in some way to measure the trustworthiness of the principal, at least for the purposesof the system concerned.

5.2.1. The Watchdog and Path rater Mechanisms:

Like the DSR routing protocol, the Watchdog mechanism makes use of passive observations. Therefore, if a node maintains a buffer containing packets it has sent toa neighboring node, then, using passive acknowledgements, the node can determine whether this neighbor has forwarded the packets. If a packet in the bufferremains unacknowledged for a certain period of time, i.e. it has not been forwarded, then a failure count for that neighbor is incremented. If the failure count exceeds a threshold, then the node sends a notification to the source of the packet identifying the selfish node.

The Pathrate mechanism operates only with source routing based protocols such as DSR, and is essentially a reputation system. A node assigns a null rating of 0.5 for each node connected to the network, derived fromthe source routes accumulated through route discovery.

The ratings of nodes on actively used source routes are increased by 0.01 every 200 ms, up to a maximum of 0.8. When a link break occurs, the node upstream of the break can send a route error message back to the source. On receipt of a route error message, the ratings of the nodes downstream of the route error originatorare decreased by 0.05, unless the rating is already 0 or less, in which case the rating is left unchanged1. If a notification of selfishness is received about a node, then the rating of that node is assigned a value of –100. All negative ratings are either increased slowly, or reset tozero after a specific period of time, in order to allow a selfish node to recover. When a node has multiple paths to the same destination, it can calculate the mean average of the ratings of each path, in order to determine which path is most likely to offer successful delivery of traffic.

5.2.2. An Overview of CORE:

Any member in Wireless Sensor Network not contributing will find their reputation worsening until they are gradually excluded from the operation of the network because of their bad reputation.

CORE defines two types of reputation, namely subjective and indirect, both of which are calculated for each function being observed. A node maintains the reputation of each neighbor node for each of a range of functional behaviors. The two types of reputationvalues are computed as follows:

- Subjective Reputation is based on local observations. If an observed behavior matches the expected behavior, then the observation will be deemed positive; otherwise it is deemed negative.
- When updating a reputation value, greater weight is given to past behavior than current behavior;
- placing more weight on past observations prevents subjective reputation being influenced by sporadic behavior.

To be able to perform observations reliably is ofextreme importance to the CORE scheme, andthe authors have suggested the Watchdog mechanism based on promiscuous observation The expected result of the current operationis stored in a buffer until a matching observation is made.

While the expected result is still present in the buffer, the reputation for the observed function is gradually decreased.

6. Performance and simulation study of the proposed DITD Model

There are two main approaches to evaluate routing applications for mobile ad hoc networks: simulations and real test beds [25],[26]. Real test beds can provide realistic results. However, they are impractical to set up. A real test bed, for a large network of nodes would requires 50 nodes in operation which is considerably costly. It is also difficult to compare different protocols because of the difficulty in repeating test conditions, such as mobility and erratic wireless connectivity. Therefore, real test beds are logistical unfeasibly. Currently, simulations are widely used to compare proposed routing protocols. Simulation packages like ns2 and [25],[6] provide an environment to design and compare proposed and existing protocols. The majority of literature on this subject use ns2 as its enhanced functionality is suitable for wireless scenarios. The ns2 network simulator was selected to perform a simulation study for the DITD model.
This section presents the effects of adding the security functionality, proposed by the DITDmodel,to the AODV routing protocol. This functionality includes a certificate distribution mechanism and a trust evaluation mechanism. The environment investigated is a large mobile ad hoc network which uses an on-demand routing algorithm. We use subsection 6.1 to: describe the simulation environment, discuss the simulation scenario, and introduce the traffic and mobility models. The performance metrics used to analyze the simulated routing protocols. Where a comprehensive simulation study is presented. This is done by comparing the proposed DITD model with the AODV routing protocol. Results are presented in simple line graphs and discussed accordingly.

6.1. Simulation setup

The goal of the simulation experiments is to measure the proposed routing protocol's performance to a changing network topology and network conditions. To measure this, protocols are simulated at varied mobility conditions. A comprehensive simulation study ispresented of the proposed security scheme for mobile ad hoc networks implemented on the network layer. A summary of the simulation set used in our study is given in Table-1.

6.1.1. Simulation Scenario

The network was set up with 50 wireless nodes allowing data communication to occur in a peer-to-peer manner. Nodes are mobile in a rectangular space of 1500m x 300m and the simulation is run for 900 seconds. A rectangular area is preferred to a square area as longer routes can be expected. Nodes were configured to use the 802.11b standard communicating over wireless channels with a two-ray ground radio propagation model with a bandwidth of 2Mbps and a nominal transmission range of 250m.

6.1.2. Traffic Model

Traffic was simulated using a constant bit rate (CBR) traffic generator which models UDP traffic. TCP traffic was not used because it uses its own flow control mechanism which schedules data packets based on the network's ability to carry them. CBR traffic is more useful for a routing protocol analysis as it allows the routing protocol to manage the flow of traffic. All traffic is started within the first 180 seconds of the simulation. Simulations were performed with data packets sizes of 64, 256, 512 and 1024 bytes. At higher data packet sizes traffic congestion causes a few nodes to drop most of their received packets, this was observed from test simulation runs. A data packet size of 64 bytes was selected for the simulation analysis. The focus of the simulation study is to compare the performance of routing protocols against changing topology and as no

load balancing is employed in any simulated protocol, congestion is factored out by selecting a lower data packet size. The traffic analysis model is consistent with routing protocol analysis in [26]. For topology analysis the traffic load is fixed with a rate of 4 packets per second.
The maximum number of connections is set to 30 connections with a traffic model with 20 sources.

6.1.3. Mobility Model

A modified "random waypoint" mobility model was used to prevent mobility concerns highlighted in [25]. The modified random waypoint model improves upon the standard model by selecting a speed which is between 10% and 90% of the given maximum speed. This addition provides a more balanced mobility and prevents extreme drops in speed during simulation.
Changing network topology is simulated based on network participant speed. The maximum speed was varied from 0 to 30m/s with 6 different mobility patterns (0.1, 1, 5, 10, 20 and 30m/s)for two different pause time scenarios, 0 and 250 seconds, representing a network with continuous motion and a partially stable network.

6.2. Performance metric

The following quantitative metrics are used to analyze the performance of the routing protocols in mobile ad hoc networks.

6.2.1. Packet Delivery Ratio

The packet delivery ratio (PDR) represents the percentage of data packets that are successfully received by their intended destination. This metric is also known as throughput and isconsidered a measurement of the effectiveness of a routing protocol.

Simulation Scenario	
Physical and MAC model	IEEE 802.11b standard
Nominal bit rate	2Mbps
Transmission Range	250m
Number of nodes	50 nodes
Simulation duration	900 seconds
Simulation area	1500m x 300m
Traffic Model	
Traffic type	CBR
Data packet size	64 byte
Traffic rate	4 packets per second
Traffic started	0 – 180 seconds
Number of connections and sources	30 and 20
Mobility Model	
Model	Random Waypoint
Max speed	0.1 , 1, 5, 10, 20, 30

m/s	
Pause time	0 and 250 seconds

Table 1. Simulation Setup for varied topology

The equation for PDR is:

$$\text{PDR \%} = \frac{\sum_1^n CBRrec}{\sum_1^n \text{CBRsent}} \times 100$$

where $\sum_1^n CBRrec$and$\sum_1^n$ CBRsentare the number of CBR data packets received and sent respectively.

6.2.2. Routing Overhead

A routing protocol uses control packets to establish routes on which data packets are transmitted. Control packets are separate from data packets but share the same communication channel. Due to the lack of channel capacity in mobile ad hoc networks a large number of control packets can result in poor network performance. Key management would require additional control packets to achieve key management functionality this will be reflected in the simulations. The routing overhead is also known as a routing protocol's internal efficiency and will represent the number of control packets used for a given protocol.

6.2.3. Average End-to-End Delay

This is a qualitative measurement of the delay of data packets. The average end-to-end delay of a data packet is the time from which it is created at the source and when it arrives at the intended destination. The delay includes propagation and queuing delay. Delay can be caused by a high number of control packets propagating in the network or a high computational overhead for the given protocol. The average end-to-end delay is calculated as follows,

$$\text{End to End Delay} = \frac{\sum_1^n(\text{CBR\_send\_time} - \text{CBR\_recv\_time})}{\sum_1^n \text{CBRrec}}$$

where CBR_send_time and CBR_recv_time represent the record times that a CBR data packet was sent and received.

6.3.DITD simulation

6.3.1. Implementation

A Linux based server was set up to run the Network Simulator ns-2.31. A routing protocol was designed in C++ based on the AODV routing protocol available in the ns-2.31 package. The routing protocol DITD is programmed as a routing agent class. The routing agent handles the establishment of routes, certificate distribution and trust evaluation. Modifications are made to the AODV routing agent at the Recv_Request, Send_Request, Recv_Reply, and Send_Reply functions. These modifications allow for the distribution of separate certificate packets, triggered by the routing packets. The routing agent's packet header was modified to include a certificate control packet Cert-S. The size of the certificate included is 450 bytes which correlates with experiments in [21].

The size of the certificate control packets is increased resulting in an effective delay in communication simulating the transfer of actual certificates. The authors of [27] use a similar approach to simulate the effect of security processing. A certificate table is included at each node Cartable which is updated by certificate control packets. The certificate table is linked to the routing table and each node is responsible for managing its own certificate table.

The trust evaluation scheme assumes that monitoring trust evidence is available. Routing control packets are modified to include an associated trust variable. As each routing packet propagates through the network, the trust of the specific route is calculated and stored in the routing table of each node. Implicit trust revocation and trust path selection is performed at Recv_Request and Recv_Reply functions respectively.

A simulation*tcl* file is written to setup the mobile ad hoc network's desired simulation scenario, traffic and mobility model. The trace support files in ns-2.31 were modified to support the DITD routing agent allowing the inclusion of certificate control packets and trust information. As a result the output trace and *nam* files reflect the operation of the DITD routing agent. AWK, an extremely versatile programming language for UNIX based systems, was used to write script files to analyze the trace data and provide the measured performance metrics. Finally UNIX based shell script files were written to allow for multiple iterations and simulation scenarios to be run simultaneously resulting in over 1000 simulation runs and 430 GB of data analyzed and presented in simple line graphs.

6.3.2. DITD Performance Results

The DITD model is compared with the AODV routing protocol. Further comparisons are presented against a conventional approach to key distribution. The simulation scenario which is used throughout the simulation study. The traffic model simulates a moderate traffic load at a rate of 4 packets per second. The effects of changing topology are investigated by varying the node speed for a continuously moving network and a partially stable network. The simulation results were averaged over 10 speeds per scenario, resulting in a total of 360 iterations for the speed analysis.

6.3.2.1.Packet delivery

The packet delivery results for the AODV and DITD routing protocols are presented in Figure 5 and Figure 6. Figure 5 represents a simulation environment with a pause time of 0 seconds. This represents a network of nodes that are continually moving, while Figure 6 represents a partially stable network. The observation is made that as the speed increases both protocols throughput decreases. At high speeds the network topology changes rapidly causing breakages in routing links. The reduction in packet delivery at high speeds is because both protocols will drop data packets as a result of increased routing breakages. The curves for the AODV and DITD packet delivery ratio have similar shapes. This is expected because the DITD model is based on the AODV model. In Figure 5 the DITD model shows a 0–10% reduction gap in packet delivery when compared to the AODV model. The gap increases uniformly as the speed increases leveling at 10% for speeds of 20 m/s and higher. Similarly for the more stable network, presented in Figure 5, there is a reduction in packet delivery ratio of 0-5% when compared to the AODV model. The stable network in Figure 5 shows better performance at higher speeds because the number of route link breakages is reduced as a result of a larger pause time.

A large pause time represents a network that will move at a given speed then pause in a fixed location for a set amount of time. During this time routing link breakages are not expected until movement commences again. The reduction in packet delivery ratio of DITD, when compared to AODV, can be attributed to the additional certificate packets being distributed and handled by the routing agent. The packet queue for the routing protocol has a limited capacity and when it is overloaded, packets are dropped. This will cause a resultant drop in throughput.

The DITD model optimizes its throughput by processing the routing and certificate control packets independently of each other. A certificate distribution scheme would expect a severe

reduction in performance due to an excessive number of packets being transmitted in the network or the additional size of the control packet. A conventional certificate distribution scheme, suggested as a possible solution in [29], simply includes the source certificate in the request packets RREQ and the destinations certificate in the reply packets RREP. This method was implemented as a separate routing agent AODV-cert in ns2.

A similar method is suggested in [29]. Implementation includes increasing the packet size of the routing control packets to include a 450 byte certificate. This effectively increased the regular 56 byte AODV route control packets to 506 bytes. Such an approach would result in the simplest method of certificate distribution but transmitting 450 bytes more data per control packet would severely reduce the network performance.

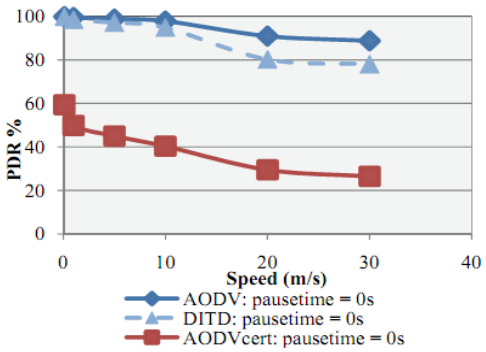

Figure5. Packet Delivery Ratio for highly mobile network (0 second pause time)

The AODV-cert routing agent was simulated under the same simulation conditions as AODV and DITD, and the packet delivery ratio is presented in Figure 7 and Figure 8. It can be observed that the packet delivery ratio is severely less than both the AODV and DITD model. For a pause time of 0 seconds, there is an average gap of 55% between AODV-cert and AODV and an average gap of 49% between AODV-cert and DITD. Similar results are observed for the stable network in Figure 9. This simulation shows that DITD optimizes the distribution of certificates by sending them as separate certificate control packets independent of the route control packets. The certificate control packets are processed independently of the routing packets, allowing concurrent processing in a fully distributive system. The operation of DITD allows for certificate distribution with minimal effect upon the routing procedure. During this time routing link breakages are not expected until movement commences again.

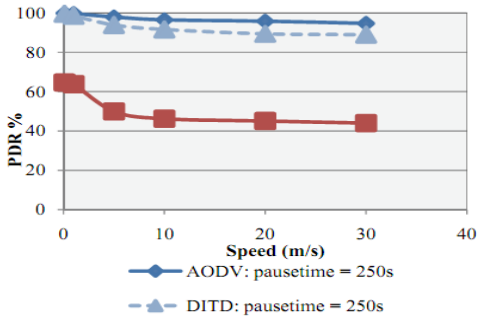

Figure6. Packet Delivery Ratio for partially stable network (250 second pause time)

The reduction in packet delivery ratio of DITD, when compared to AODV, can be attributed to the additional certificate packets being distributed and handled by the routing agent. The packet queue for the routing protocol has a limited capacity and when it is overloaded packets are dropped. This will cause resultant drop in throughput. The DITD model optimizes its throughput by processing the routing and certificate control packets independent of each other.

A certificate distribution scheme would expect a severe reduction in performance due to an excessive number of packets being transmitted in the network or the additional size of control packet. A conventional certificate distribution scheme, suggested as a possible solution in [21], simply includes the source's certificate in the request packets RREQ and includes the destination's certificate in the reply packets RREP. This method was implemented as a separate routing agent AODV-cert in ns2. A similar method is suggested in [29]. Implementation includes increasing the packet size of the routing control packets to include a 450 byte certificate. This effectively increased the regular 56 byte AODV route control packets to 506 bytes. Such an approach would result in the simplest method of certificate distribution but the result of transmitting 450 bytes more data per control packet would severely reduce the network performance.

The AODV-cert routing agent was simulated under the same simulation conditions as AODV and DITD and the packet delivery ratio is presented in Figure 6 and Figure 7. It can be observed that the packet delivery ratio is severely less than mobile ad hoc networks. A high speed network is described by a maximum node speed of 20 and 30 m/s. This simulates mobile units travelling at a maximum speed of 70–100km/h which is typical of mobile military vehicles. Mobility aids the distribution of certificates as nodes come in close contact with each other and are able to establish direct trust relations reducing end-to-end certificate distribution. These benefits are similar to [19] solution which relies upon mobility to establish trust in a localized manner [20].

[20]solution is aided by mobility but is also dependent upon mobility for trust relations to be established. Because of this dependency, a period of weakened security is expected as nodes exchange certificates. DITD does not only distribute certificates in a localized manner but Figure 8 shows that the DITD model has a 0 - 3% reduction in throughput for low speed mobile ad hoc networks where nodes move at a maximum speed of 0–10 m/s. This type of networks is typical of infantry units or a *nam* the ground scenario. DITD allows for mobility to aid the distribution of certificates but not relying upon mobility for throughput success. This allows DITD to operate successfully in slow moving and stationary type networks. The packet delivery ratio results show that DITD provides certificate distribution at a low performance cost for high speed networks and for low speed networks.

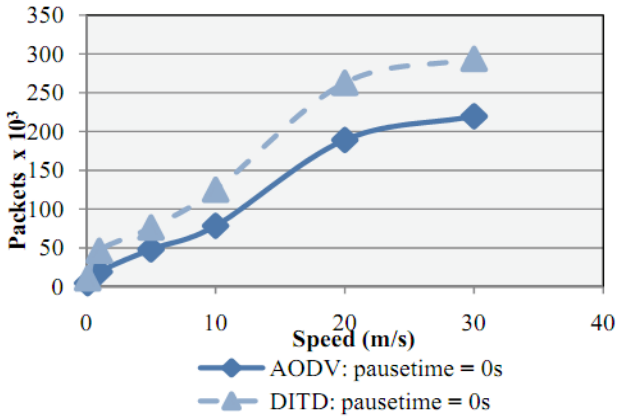

Figure 7: shows that the DITD model has a 10% reduction in throughput for high speed

6.3.2.2.Control Packet Overhead

The control packet overhead presents a comparison between the AODV and DITD models. The overhead is presented in terms of the number control packets. The AODV model will have only routing control packets while the DITD model will have both routing and certificate packets. The results are presented in Figure 8 for a highly mobile network with pause time of 0 seconds and a partially stable network with pause time of 250 seconds. The DITD model aims to distribute certificates while routes are discovered and a resultant packet overhead is expect.

AODV and DITD are similar in shape and it is observed that the number of control packets increases as the speed increases. As the speed increases the topology of the network changes more rapidly causing routing link breakages and forcing nodes requesting communication to re-establish routes by send new route request messages. For a partially stable network presented in Figure 8 the effects of speed are reduced. This confirms that a larger pause time provides a more stable network. Figure 7 and Figure 8 show a consistent control packet overhead for the DITD model. It is observed that the gradient of DITD's packet overhead decreases as speed increases. This is because mobility aids certificate distribution and as the speed increases less certificate control packets are required. For example in Figure 7 at the low speed of 1 m/s there is a 132% increase in the number packets when compared to the AODV protocol. This overhead decreases for higher speeds showing a comparative 38% and 33% packet overhead for speeds of 20 m/s and 30 m/s respectively. This confirms that mobility aids certificate distribution.

A standard AODV request message is 48 bytes and a reply message is 44 bytes. The DITD model uses request message of 60 bytes and reply messages of 56 bytes. Therefore, DITD increases the routing control packet size by 12 bytes. DITD's routing control packets contain trust associated variables and flags to trigger back-tracked certificate distribution. The DITD certificate control packets are 508 bytes in size as they included a 450 byte certificate. It is noted that making the routing and certificate control packets separate and independent from each other has a greater impact on reducing the per byte packet overhead. This independency allows for concurrent processing of packets which is optimal in a fully distributive ad hoc network.

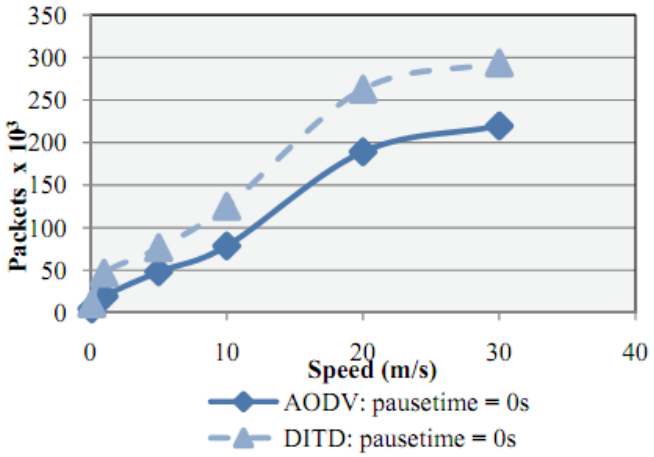

Figure 8: Control packet overhead for highly mobile network (0 second pause time)

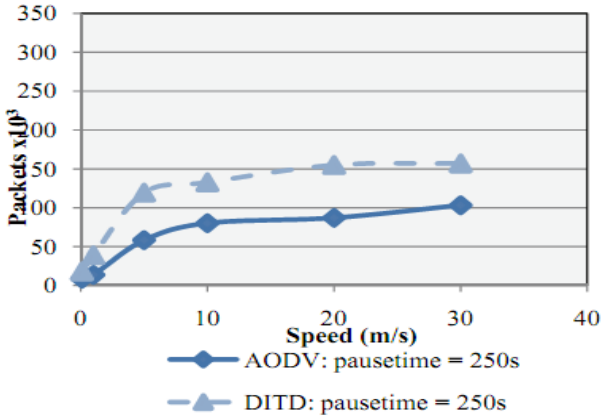

Fig.9: Control packet overhead for partially stable network (250 second pause time)

6.4. Trust Evaluation Results

In order to test the performance of the security evaluation scheme, a black hole attack was simulated to show that DITD's security evaluation scheme excludes malicious nodes from trust and route establishment protecting the network from black hole type attacks. A black hole adversary model was designed on the ns-2.31 link layer (LL) which lies below the routing layer. Modifications were made to the link layer agent ll.cc to simulate a black hole attack. Each packet sent by the routing layer is checked at the link layer, the adversary model silently drops all data packets while still allowing routing packets to be passed. This creates the effect of a black hole attack. A second black hole adversary model was implemented which includes a rushing type attack.

The rushing attack was implemented by allowing adversary nodes to forward routing packets immediately, removing the small jitter delay that AODV implements. AODV uses this small delay to reduce the number of collisions and ensure the shortest path is selected. The rushing attack gives an adversary node a time advantage over normal nodes resulting in the adversary node becoming part of considerably more routes.

The same simulation scenario and traffic model was used to analyze the black hole attack. The mobility was fixed with a pause time of 0 seconds and three speeds were investigated (0.1m/s, 5m/s and 20m/s). A 50 node network was simulated with 6 different attack scenarios. The attack scenarios were created by varying the number of black hole adversary nodes added by 0 to10. Figure 11 shows the *nam* simulation file for a simulation scenario with 10 adversary nodes. Each scenario was averaged over 10 seeds resulting in 720 iterations for the security evaluation scheme analysis. The black hole attack aims to drop data packets and reduce the networks throughput.

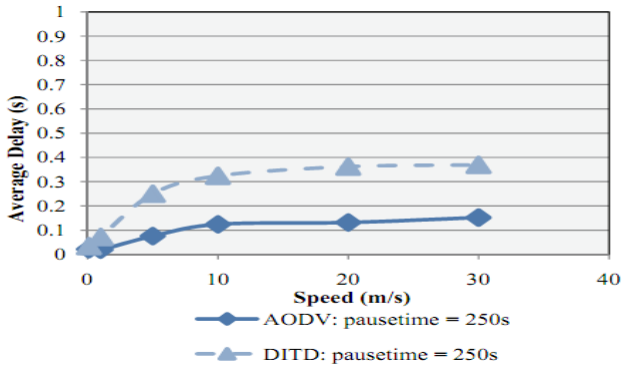

Fig. 10: Average end-to-end delay for partially stable network (250 second pause time)

The effects of a black hole and rushing attack are analyzed using the packet delivery ratio performance metric.

A black hole type problem is implemented to simulate the success of DITD's security evaluation scheme. The scenario assumes weighted nodes carry a security metric which identifies fault detection or data transmission errors carried out by a monitoring system at each node. An example of such a system is found in [29]. The weighted nodes are used to establish a weighted trust graph where each edge or route carries a trust calculated by DITD's security evaluation scheme. The effects of the black hole attack upon AODV and DITD are compared in Figure 10 and Figure 11. It is observed that as the number of adversary nodes increases the packet delivery ratio for the AODV model decreases. The AODV model is vulnerable to black hole attacks and in the presence of 10 adversary nodes the packet delivery ratio is below 65%. The reduction in throughput is expected as more data packets will be dropped by the presence of many adversary nodes.

DITD avoids the adversary nodes by implicitly excluding these nodes during route establishment. The success of the protocol at low speeds is presented in Figure 12 and it is observed that even in presence of 10 adversary nodes the packet delivery ratio is not less than 90%. Figure 11 presents the success of the DITD model at a higher mobility of 20m/s. The DITD model prevents the severe effects of black hole attacks showing better results when 4 and greater than 4 adversary nodes are present. There is approximately a 10% decrease in packet delivery ratio when compared to the low mobility scenario in Figure 12.

This reduction in packet delivery ratio is attributed to the increase in link breakages apparent at higher speeds and the overhead incurred from the certificate exchange protocol. The results of DITD correlate to the packet delivery ratio at 20m/s in Figure 5. A rushing attack was included for the simulations presented. An adversary node equipped with a rushing type attack will participate in more routes maximizing the effect of its attack. Figure 11 and Figure 12 show that when adversary nodes employ a rushing attack the effects of the black hole attack are maximized. The packet delivery ratio of the AODV protocol is dropped to 40% when 10 adversary nodes are present. This is considerably less when compared to the 60-65% packet delivery ratio that AODV experiences under the same conditions with a standalone black hole attack. The results of DITD under rushing attacks are unnoticeable when compared to DITD with no rushing attacks. For low speeds, DITD provides a throughput rate of above 90% even in the presence of 10 adversary nodes.

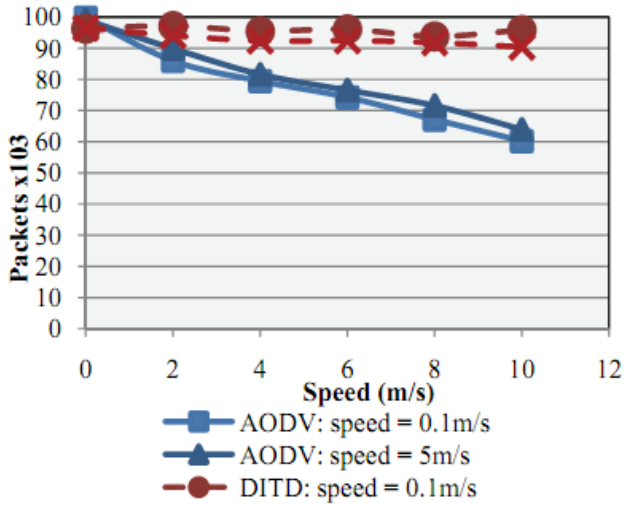

Figure 11: Packet Delivery Ratio for slow moving network under black hole attack

DITD provides a security scheme that excludes malicious nodes from participating in trusted routes, therefore preventing black hole attacks and a number of other attacks targeting the network layer. The inclusion of this trust evaluation scheme allows the distribution of certificates to operate in the most trusted routing environment.

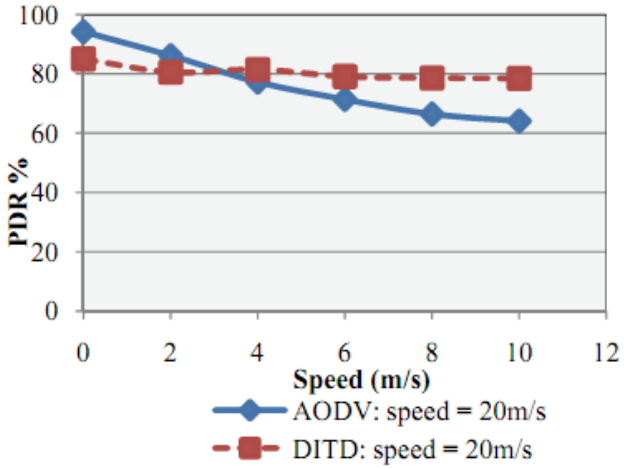

Figure12: Packet Delivery Ratio for fast moving network under black hole attack

7. CONCLUSION

This paper proposed the methods to analyze the process of trust establishment in distributed networks. he tools for performing the analysis were implemented, and validated by simulations. The proposed analysis methods were utilized to solve an important research problem: quantitative comparison among different trust models. In the future, we will exploit more applications of the analysis tool, such as understanding the effects that application context has upon trust establishment, and guiding the design of better trust establishment methods.

References

[1] Y.-C. Hu, A. Perrig, and D. B. Johnson, "Ariadne:: A Secure On demand Routing Protocol for Wireless Sensor Network Networks". Proceedings of International Conference on Mobile Computing and Networking, pp. 12-23, Atlanta, USA, 2002.

[2] P. Papadimitratos and Z. J. Haas, "Secure Routing for Mobile Wireless Sensor Network Networks". Proceedings of SCS Communication Networks and Distributed Systems Modeling and Simulation Conference, USA, 2002

[3] L. Buttyan and J. Hubaux, "Nuglets: A Virtual Currency to Stimulate Cooperation in Self-organized WireLess Sensor Network Networks". Swiss Federal Institute of Technology, Lausanne DSC/2001/001, 2001.

[4] S. Zhong, J. Chen, and Y. R. Yang, "Sprite: A Simple, Cheat-proof, Credit-based System for Mobile Ad-hoc Networks". INFOCOM 2003, pp. 1987 - 1997, 2003.

[5] Y. Liu and Y. R. Yang, "Reputation Propagation and Agreement in Mobile Ad-hoc Networks". Proceedings of IEEE Wireless Communications and Networking (WCNC 2003), New Orleans, USA, pp. 1510-1515, 2003

[6] S. Yan Lindsay, Y. Wei, H. Zhu and K. J. R. Liu, "Information Theoretic Framework of Trust Modeling and Evaluation for Wireless Sensor Network Networks". IEEE Journal on Selected Areas in Communications, 24(2), pp. 305-317, 2006

[7] L. Zhou and Z.J.Haas, "Securing Wireless Sensor Network Networks". IEEE Network, 13(6), pp. 24-30, 1999

[8] H. Luo, P. Zerfos, J. Kong, S. Lu and L. Zhang, "Self-securing Wireless Sensor Network Wireless Networks". IEEE ISCC, 2002

[9] Aldar C-E Chan, "Distributed Symmetric Key Management for Mobile Wireless Sensor Network Networks". INFOCOM 2004, China, pp. 2414-2424, 2004.

[10] V. Balakrishnan, V. Varadharajan, U. K. Tupakula, and P. Lucs, "Trust Integrated Cooperation Architecture for Mobile Ad-hoc Networks". Proceedings of 4th IEEE International Symposium on Wireless Communication Systems (ISWCS 2007), Trondheim, Norway, 2007

[11] V. Balakrishnan, V. Varadharajan, P. Lucs, and U. K. Tupakula, "Trust Establishment Secure Mobile Wireless Sensor Network Routing". Proceedings of 21st IEEE International Conference on Advanced Information Networking and Applications Workshops (AINAW 2007), Canada, pp. 27-33, 2007

[12] V.Balakrishnan, V. Varadharajan, U. K. Tupakula, and P. Lucs, "Trust and Recommendations in Mobile Wireless Sensor Network Networks". Proceedings of 3rdInternational Conference on Networking and Services (ICNS 2007), Athens, Greece, pp. 64-69, 2007

[13] V. Balakrishnan, V. Varadharajan, and U. K. Tupakula, "Fellowship: Defense against Flooding and Packet Drop Attacks in MANET". Proceedings of 10th IEEE/IFIP Network Operations and Management Symposium (NOMS 2006), Vancouver, Canada, pp. 1-4, 2006

[14] V. Balakrishnan, and V. Varadharajan, "Fellowship in Mobile Wireless Sensor Network Networks". Proceedings of 1st IEEE International Conference on Security and Privacy for Emerging Areas in Communications Networks (SecureComm 2005), Athens, Greece, pp. 225-227, 2005

[15] V. N. Padmanabhan and D. R. Simon. Secure traceroute todetect faulty or malicious routing. ACM SIGCOMM ComputerCommunications Review, 33(1):77–82, Jan 2003.

[16] B. Parno, A. Perrig, and V. Gligor. Distributed detection of nodereplication attacks in sensor networks. In SP '05: Proceedingsof the 2005 IEEE Symposium on Security and Privacy, pages49–63, Washington, DC, USA, 2005. IEEE Computer Society.

[17] K. Paul and D. Westhoff. Context aware detection of selfishnodes in DSR based ad-hoc networks. In Proceedings of theIEEE Global Telecommunications Conference, GLOBECOM'02, Taipei, Taiwan, November 17-21, 2002, volume 1, pages186–190. IEEE Press, Nov 2002.

[18] B. Raghavan and A. C. Snoeren. Priority forwarding in Wireless Sensor Networknetworks with self-interested parties. In Proceedings of the FirstWorkshop on Economics of Peer-to-Peer Systems, Berkley, CA,June 5-6, 2003, June 2003.

[19] M. G. Reed, P. F. Syverson, and D. M. Goldschlag.Anonymousconnections and onion routing. IEEE Journal on Selected Areasin Communications, 16(4):482–494, May 1998.

[20] Zapata M.G., "Secure ad hoc on-demand distance vector routing," SIGMOBILE Mob. Comput.Commun.Rev., vol. 6, pp. 106-107, 2002.

[21] Theodorakopoulos G. 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

[22] Kschischang F.R., B. J. Frey, and H.-A. Loeliger, "Factor graphs and the sum-product algorithm," IEEE Transactions on Information Theory, vol. 47, pp. 498-519, 2001.
[23] Mohri M., "Semiring frameworks and algorithms for shortest-distance problems," J. Autom. Lang. Comb., vol. 7, pp. 321-350, 2002
[24] Kiess W. and M. Mauve, "A survey on real-world implementations of mobile ad-hoc networks," Ad Hoc Netw., vol. 5, pp. 324-339, 2007.
[25] Zeng X., R. Bagrodia, and M. Gerla, "GloMoSim: a Library for Parallel Simulation for Large-scale Wireless Networks," in proc. 12th Workshop on Parallel and Distributed Simulations, 1998.
[26] J. Broch, D. A. Maltz, D. B. Johnson, Y.-C. Hu, "A performance comparison of multi-hop wireless ad hoc network routing protocols," in Proceedings of the 4th annual ACM/IEEE international conference on Mobile computing and networking Dallas, Texas, United States: ACM, 1998.
[27] Navidi W., "Stationary Distributions for the Random Waypoint Mobility Model," IEEE Transactions on Mobile Computing, vol. 3, pp. 99-108, 2004.
[28] Stephan Eichler C.R., "Challenges of Secure Routing in MANETs: Aimulative Approach using AODV-SEC," in Mobile Adhoc and Sensor Systems (MASS), 2006 IEEE International Conference on, 2006.
[29] B. Awerbuch, D. Holmer, C. Nita-Rotaru, and H. Rubens, "An on-demand secure routing protocol resilient to byzantine failures," in Proceedings of the 1st ACM workshop on Wireless security Atlanta, GA, USA: ACM, 2002.

Authors

Mohammad Reza KaghazGaran

He was born in Mashhad-Iran and B.Sc. Software Computer Engineering and graduated on June 2011of Islamic Azad University of Mashhad. His researches are Wireless and recently Vehicular Network and Bioinformatics.

Afsaneh KaghazGaran

She was born in Mashhad-Iran and received B.Sc. in Nursing On 1994 Of Islamic Azad University, Branch of Mashhad. Her researches are Bioinformatics and Medical & Paramedical. His interests in issues of network and computer network and connections between the medical and paramedical with computer network.