Secured Data Forwarding Routing Protocol (SDFRP) For Heterogeneous Mobile Ad Hoc Networks

A.K.Ashfaq Ahamed, Dr.M.Anand Kumar, Dr.B.L.Shivakumar
Assistant Professor, Department of Computer Applications, Kongunadu Arts and Science College, Coimbatore, India.
Associate Professor, Department of Information Technology, Karpagam University, Coimbatore, India.
Principal, Sri Ramakrishna Polytechnic College, Coimbatore, India.

Abstract-Secured data forwarding is an overwhelming task among the mobile ad hoc networks as the wireless transmission medium is more vulnerable to attack. This research work focuses on network and attack model which takes into account of different valid scenarios (that will probably prone to attacks) while communications are carrying out collisions, channel error or mobility and also exist situations mainly, malicious / anomalous behaviors, security attacks and more. Routing overhead, throughput, packet delivery ratio and delay metrics are chosen to conduct performance analysis under two scenarios namely velocity and density. Simulations are carried out using NS2 and the proposed security strategy performs better.

Key words: MANET, SDFRP, TCP.

1. Introduction
There are several attacks which can affect the performance of operation in MANETs. Some of these attacks are insider (happened from internal authorized nodes which are malicious or compromised nodes) and others are external attacks (occurred from outsider nodes which do not belong to a specific MANET). These attacks can be classified as passive attacks (that eavesdropper does not interact directly with authorized nodes or affect intentionally the channel between them; but he can capture transferred information between those nodes to analysis or to take an action) and active attacks (here eavesdropper tries to masquerade himself as a legitimate node to redirect the path of transmitted data; and a breakdown in the transmission channel between authorized nodes can be done) [4]. The following section will provide some attacks which can face MANETs [3]:

(1) **Message spoofing**: the eavesdropper node sends false messages to other nodes to deceive them and disseminate wrong information.

(2) **Message replay attack**: the malicious node replays send past messages in order to jam traffic.

(3) **Integrity attack**: the misbehaved node can change the context of messages sent by legitimate nodes or by itself mislead the other nodes (receptionists) from knowing the original data or the real sender of this data.

(4) **Impersonation Attack**: the eavesdropper node claims that it is a legitimate node to send false messages to other nodes and remote nodes.

(5) **Denial of Service (DoS) attack**: the misbehaved node sends irrelevant or unimportant messages to reserve large bandwidth of the communication channel and consume more resources of other nodes.

(6) **Movement tracking**: the misbehaved node can access some information of other nodes which helps to track their position and speed. Hence, it can detect future behavior of those nodes and affect their transmission performance.

Due to the nature of MANETs that they are self-organized networks, some security requirements should be found as follows [1, 2]:

- Data Authentication and Integrity
- Data Confidentiality
- Node Privacy and Anonymity
- Access Control
- Data Non-Repudiation
- Integrity
- Node ID Traceability
- Scalability [3]
- Efficiency and Robustness
- Forgery
- Availability
- Anti-Jamming
- Impersonation
- Resistance against In-Transit Traffic and On-Board Tampering

Some classifications of attacks in MANETs were established such as [5] according to attacks’ features.
1.1. Attack nature

Some malicious attacks (false information is spread about unreal events or wrong identities of a group of nodes in a MANET) cannot be detected due to their nature. Malicious nodes in MANET can spoof itself like a legitimate node that other communicating nodes cannot observe them although these nodes have correct information (location and their inter-distances) about themselves. As a Consequently, some attacks such as Sybil attacks cannot be detected easily, and concerns should be established to build a strong trust negotiation depending on dynamic behavior of MANETs.

[Diagram: Misbehaving node inside MANET]

1.2. Attack target

The eavesdropper nodes are strongly recommended to have attack target when they can communicate over long distances. These nodes have more flexibility to send false announcements and information to other nodes at long distances. Hence, detecting such behaviors is harder than a local eavesdropper like a man in the middle attacks. Accordingly, some configuration systems such as hierarchy systems should be used to describe some authenticated remote nodes which will authorize any new communicating node outside its local MANETs.

1.3. Attack scope

Attacks can be classified according to its affecting area such as limited and extended attacks. Limited attacks mean that the number or the area containing victim nodes (nodes handle uncorrected information due to malicious nodes) is small. On the other side, extended attacks mean that the effect of malicious behavior has a great value on a large number of communicating nodes or happens in a large area of a MANET.

1.4. Attack impact

Attacks can also be classified due to their impacts on nodes in MANETs. The first impact is that attacks are undetected because communicating nodes are isolated or many malicious nodes around them. The second impact is that attacks may be detected but they are not completely corrected due to insufficient information gathered by nodes. Consequently, the communicating nodes will receive incorrect data and may remain wrong for some time. Finally, attacks can be detected and corrected by nodes since they are connected to a large number of honest remote nodes. Hence, any received data can be checked and identified by those remote nodes to find corrected or uncorrected data and it is shown in Fig.1.

2. Related Works

In MANETs, nodes are receptive to being captured, compromised, and hijacked because they are unit capable of roaming independently. Since tracking down mobile nodes is difficult, attacks by compromised nodes are far more damaging and harder to detect [6]. For limited energy budget in most mobile nodes, the energy depletion phenomenon could be deteriorated by roaming attacking nodes. One potential RREQ flooding attack in MANETs was presented by Yi et al. [7]. The attacking pattern by RREQ flooding attack firstly selects fraudulent IP addresses which are not inside the legal IP domain defined/configured in the target MANET. Then the malicious node issues RREQ packets containing such an out-of-domain IP to call for relay service from its neighboring nodes. To reduce the congestion caused by the dissemination of RREQ packets issued by all nodes in the MANET, three major controlling techniques are utilized in [8]: rate of firing RREQ packets, the waiting time for the arrival of RREP packet, and prolongation of waiting times in case of resending RREQ packet without receiving the responsive RREP packet. On controlling the rate of firing RREQ packets, it is requested that a node should not originate more than RREQ_RATELIMIT RREQ messages per second. In order to defy RREQ flooding attack in mobile ad hoc networks, Yi et al. [7] proposed the flooding attack prevention (FAP) scheme in order to defy against RREQ flooding attacks. FAP schemes consists of “Neighbor Suppression” for successfully defying the RREQ flooding attack. Neighbor Suppression mechanism is capable of enough to change the processing rule of default while RREQs arrive from neighbor mobile nodes. The authors also pointed out a hypothesis that the processing precedence of a RREQ from an exact mobile node is in inversely comparative to the arriving occurrence. The authors mentioned that exist certain apparent and inevitable impacts such as redundant rebroadcast, contention, and collision [9]. In order to resist against such storm attack scenarios, Yi et al. [7] stated a new idiom in MANETs: RREQ flooding attack. This RREQ
flooding attack is launched by attackers who would like to inject the volumes of RREQ packets with an out-of-domain IP address as its destination node. This also helps in identifying the stale routes from the new ones, thereby avoiding the formation of loops [10]. Accurate and precise malicious node exclusion mechanisms for ad hoc networks are presented [11]. A robust and distributed access control mechanism based on a trust model is proposed in order to secure the network and stimulate cooperation by excluding misbehaving nodes from the network. The mechanism divides the access control responsibility into two contexts: local and global. The local context responsibility is the neighborhood to watch and notify the global context about suspicious behavior. In its turn, the global context analyzes the received information and decides whether it punishes the suspicious node using a voting scheme. The exclusion mechanism is modeled and performs a parameter analysis. Secure neighbor discovery and wormhole localization in mobile ad hoc networks is proposed [12]. Mobile Secure Neighbor Discovery (MSND), which offers a measure of protection against wormholes by allowing participating mobile nodes to securely determine if they are neighbors, and a wormhole localization protocol allows the nodes that detect the presence of a wormhole to determine wormhole’s location. By observing all these above mentioned literatures, this work is first to secure neighbor discovery in mobile ad hoc networks and to localize a wormhole. MSND leverages concepts of graph rigidity for wormhole detection. In [13] the authors proposed secured reliable multipath routing protocol (SRMRP) using distributed trust computation and carrier sense multiple accesses with collision intimation for distributed heterogeneous mobile ad-hoc networks. The primary objective of SRMRP is to make the communication secured against the attacks. For achieving this reference based on trust security mechanism is proposed. The next objective is to provide reliable data communication in heterogeneous mobile ad hoc networks. For achieving this adaptive carrier sense, and multiple accesses with collision intimation mechanism is employed. The simulations are done in NS2. Network security has received a wide attention due to the supporting security concerns in networks[14]. This paper concerns the real time mobile ad hoc networks i.e., heterogeneous natured.

3. Proposed Work
Secured data forwarding routing protocol (SDFRP) offers every node in the network with a breadth-first spanning tree of the intact network is rooted. Breadth-first spanning tree mechanism allows the mobile nodes to occasionally broadcast the tree structure in each cycle. Depending upon the gathered information from neighbor nodes through the most topical steps, a mobile node will probably increase and revise its information about the ad hoc networks topology by constructing a deeper and more recent breadth-first spanning tree. This vital information will be distributed to its neighbors in the next round of operation. Inversely, when a neighbor mobile node is lost due to its range, a process is triggered in order to remove its relevant information from the topology repository maintained by the detecting mobile nodes in the ad hoc network. The proposed work develops a network and attack the model by keeping into account of various justifiable situations while communication happens with collisions, channel error and also mobility. In addition, the attack model portrays malicious behaviors among mobile nodes by knowing the way in which such malicious nodes will affect the performance of the overall retransmission process.

The packet forwarding process an ad hoc network scenario entails with several steps. When a data packet is rightly received by a mobile node in the ad hoc network, there are various consecutive events that will mandatorily happen for the packet to be forwarded. They are listed out below:

Destination Event: In this event, the particular mobile node is considered as not the final destination node of the data packet.

Route Event: In this event, the node consists of valid route in order to relay the packets towards the destination node.

Drop Event: In this event, the stipulated mobile node is considered not a malicious dropper and hence it will not drop the packets.

During when all of the above said events occur, the mobile node in the ad hoc network will attempt to forward the data packet. In order to perform this above said thing, two steps are involved. Initially, the mobile node will attempt to forward a Request-To-Send (RTS) packet. Next, the mobile node will countercheck whether it gets back Clear-To-Send (CTS) packet. This CTS packet is received from the nearby mobile node that exists in the route only when the consequent RTS packet would have been reached its destination and the CTS packet is successfully received.

There is a probable occurrence that RTS packets and CTS packets can be affected by channel errors by denying them in reaching their destination mobile node. There exists another situation where a packet discarding occurs. It happens due to the mobility of mobile nodes during when they are moving out of communication range. Consequently when they are out of their transmission range they do not have adequate time for updating the routing table. This results in communication loss among the mobile
nodes. The above said scenarios will result in message losses along with dropping of RTS and CTS packets not received at the appropriate mobile nodes. In such case RTS retransmission is unavoidable. The several causes for communication link, exists to be broken, in this research it is considered that mobility as the primary factor for link breakage. When the sender mobile node acquires the wireless communication channel it transmits the desired data. This can be said as; when the data packet is forwarded by the particular mobile node the forward event will be occurred. For successful forwarding of message RTS and CTS need to be happened successfully.

3.1. Detecting malicious packet drops
In this section, a detection mechanism is proposed for packet dropping in mobile ad hoc networks scenario. In the beginning, an attack model is portrayed. Next the detection mechanism is explained. In addition to that, parameters estimation along withwindowing mechanism is given. At last, a summary is shown.

3.1.1. Attack model and scenario description
It is deemed that there are $L$ legitimate mobile nodes are placed in certain locations among the terrain regions. The nodes present in the terrain are moving in a specified speed. It is noteworthy to presume that IEEE802.11 MAC mechanism is chosen for the scenario by which RTS packets and CTS packets are employed. 802.11 Distributed Coordination Function (DCF) is present in this MAC in order to perform the aforementioned things. Hidden node terminal problem is occurred due to the mobility of the nodes and also due to the lack of carrier detection which results in lot of collisions. Mobile nodes in the ad hoc networks communicate using the protocol and it is to be noted that there are various kinds of traffic flows. Commonly it is considered that malicious mobile nodes in the ad hoc networks have same behavior as the legitimate mobile nodes have. There is an exception in that. Legitimate mobile nodes also drop received packets instead of forwarding them. It is to be presumed that an attack model with malicious mobile nodes can work in autonomous manner and do not collide with each other. It is noteworthy that attackers exist in the ad hoc networks may not cooperate themselves. There are many attack scenarios can be implemented as found in the literatures [31–34].

3.1.2. Detection approach
In this proposed research, a window based process that deemed or not a mobile node as malicious discretely overtime is presented. In this manner, a suite of network related features are taken for each mobile node in a given temporal window for the analysis. By the use of these attributes, the probability values are estimated next. To end with, a verdict about the behavior of a target node is obtained.

$$P_{DROP} = 1 - \frac{P_{FWD}}{1 - (P_{COL} + P_{MOB})}$$  \hspace{1cm} (1)

This dropping probability is consequently evaluated with predefined detection threshold called $\theta$. A condition is checked if $P_{DROP}$ is larger than this threshold and according to anomaly based approach, it can be finished off that the analyzed mobile node is malicious. Else the mobile node is considered as legitimate by the following equation.

$$node = \begin{cases} \text{malicious, if } P_{DROP} \geq \theta \\ \text{legitimate, otherwise} \end{cases}$$ \hspace{1cm} (2)

It is perceptible that the working juncture of the detection is based on the value used for the detection threshold. When $\theta$ is set with lesser value, then more malicious nodes will be detected in the ad hoc network. Also there is a possibility that more legitimate mobile nodes will be misclassified as malicious. Quite the opposite, the use of high values for $\theta$ can classify less malicious nodes.

3.1.3. Parameters estimation
There are three parameters need to be estimated such as $P_{FWD}$, $P_{COL}$ and $P_{MOB}$. $P_{FWD}$ and $P_{COL}$ applied for experimental approximation. At first, $P_{FWD}$ is calculated as the percentage of data packets forwarded by the mobile node. In this manner, IDS keep track on traffic of the analyzed mobile node in search of received data packets whose destination is not the analyzed node itself. $P_{FWD}$ is estimated using:

$$PFWD = \frac{\#DATA_{FWD}}{\#DATA_{FWD}}$$ \hspace{1cm} (3)

It is kept in mind that, only when a mobile node is not the destination node of the packet and exists a valid route, the packet will be counted as a received data packet in $\#DATA_{RECV}$. When the legitimate packet (packet which does not contain malicious data) is discarded, the proposed IDS classifiers into two possible situations such as collision and mobility. Regarding $P_{COL}$, since the associated effect is related to the traffic load, the number of RTS packets are sent by the node without a proper CTS reply ($\#RTS_{SENT} - \#CTS_{RECV}$) is computed, as well as the total number of attempts to seize the channel. As said, only those packets which are not directly related to broken links situations are taken in to account, i.e., those RTS retransmissions which do not exceed the SRL limit. In summary, an estimator for the collision
and channel error probability $\hat{p}_{\text{COL}}$ can be computed as follows:

$$\hat{p}_{\text{COL}} = \frac{\# \text{RTS}_{\text{SENT}} - \# \text{CTS}_{\text{RECV}}}{\# \text{RTS}_{\text{SENT}}}$$

Finally, $P_{\text{MOB}}$ is estimated. The proposed estimator for the probability of a broken link situation can be easily computed, since it takes one of just two values.

$P_{\text{MOB}}$ is set to 1 when the number of RTS retransmissions exceeds the SRL limit in a measuring window, since here the node considers that it does not have a connection with the next hop. The estimator is set to 0 otherwise, because the link is not considered to be down. That is, $P_{\text{MOB}} =\begin{cases} 1, & \text{if } \# \text{RTS}_{\text{SENT}} > \text{SRL} \\ 0, & \text{otherwise} \end{cases}$

Scenario 1: In this scenario, it is cogitated that the broken communication link is nearer to the source mobile node than to the destination mobile node. In this scenario, the intermediate mobile node discards the route and sends RERR (route error) message in order to vigilant its previous mobile nodes about the link failure. At this juncture, the previous nodes terminate forwarding data packets to the intermediate mobile nodes which result in retransmission of RERR messages.

Scenario 2: In this scenario it is considered, that the communication link is nearer to the destination mobile node than to the source mobile node. It is noteworthy that the intermediate node attempts to locally fix the route. So, in order to perform, it sends a RREQ packet alike the source mobile node. When the route cannot be repaired after the period, the intermediate node sends a RERR packet to its precursor mobile nodes in the ad hoc networks. It is noted that the mobile node with the broken communication link will act as a malicious node for a certain amount of duration since it continues receiving messages. Even though it can receive messages and could not forward packets. Due to the above said situations in this scenario it takes around 12 to 15 seconds to conduct route maintenance.

### 3.1.4. Improved windowing for gathering features

In this section, improved windowing for gathering features is presented. It is a mechanism applied by monitoring features. This mechanism performs by selecting certain temporal observations over succeeding non-overlapped analysis windows within a fixed time frame. On the other hand, this mechanism has two pitfalls. The first one is connected to the criteria in which the temporal window closes immediately when the transmission of an RTS packet is over. At this situation, it is impossible to conjecture whether the packet is properly replied when a collision happens due to node mobility. The next pitfall is related to collecting biased information. This biased information shows the way to inappropriate detection results. In order to surmount the above said pitfalls, in this research it is attempted to propose an event based windowing procedure rather time based one. To be precise, the features are attained for non-overlapping windows of received data packets for each mobile node in the ad hoc networks.

Hence by proposed event based windowing mechanism the above said two pitfalls are surmounted in terms of better throughput, reduced overhead and less delay.

### 3.1.5. Summary of the detection approach

For detecting whether the mobile node in the ad hoc network is $N_i$ is behaving maliciously as a packet dropper, the following are the main features

1. $\#\text{RTS}_{\text{SENT}}$: No. of RTS packets sent by node $N_i$
2. $\#\text{CTS}_{\text{RECV}}$: No. of CTS packets received by node $N_i$
3. $\#\text{DATA}_{\text{RECV}}$: No. of data packets received by node $N_i$
4. $\#\text{DATA}_{\text{FWD}}$: No. of data packets forwarded by node $N_i$
5. $\#\text{RREQ}$: Boolean attribute value is TRUE when a RREQ message has been broadcasted by node $N_i$, and FALSE otherwise.

Considering all the above things the features such as ($\#\text{RTS}_{\text{SENT}}, \#\text{CTS}_{\text{RECV}}, \#\text{DATA}_{\text{RECV}}, \#\text{DATA}_{\text{FWD}}$ and $\#\text{RREQ}$) are helpful for detecting a dropping attack, $P_{\text{DROP}}$, which decides if a node is malicious, or not, to the following expression:

$$P_{\text{DROP}} = \begin{cases} 0, & \text{if } \hat{p}_{\text{MOB}} = 1 \\
1 - \frac{\hat{p}_{\text{FWD}}}{1 - \hat{p}_{\text{COL}}}, & \text{otherwise} \end{cases}$$

The detection procedure is portrayed in the below algorithm. It is noteworthy that the detection procedure is based on an analytical model which employs simple features to carry out the detection process. The proposed mechanism has lower computational complexity in terms of overhead. In addition to that, the proposed routing mechanism reduces the large training datasets.

#### Algorithm 1: Pseudo-code for the dropping detection.

1. for each window $\omega$ in the monitoring time do
2. for each node $N_i$ in the network do
3. Obtain $\hat{p}_{\text{FWD}}$
4. Estimate $\hat{p}_{\text{COL}}$
5. Estimate $\hat{p}_{\text{MOB}}$
6: Compute $P_{\text{DROP}}$
7: if $P_{\text{DROP}} < \Theta$ then
8: if $RREQ == \text{FALSE}$ then
9: $Ni$ is legitimate during the window $\omega$.
10: else
11: $Ni$ is legitimate for every $\omega$ during $T$.
12: end if
13: else
14: $Ni$ is malicious during the window $\omega$.
15: end if
16: end for
17: end for

4. Simulation Settings

While configuring node mobility in the ad hoc networks, make use of random waypoint model to generate node movements. In the simulation, each mobile node moves randomly. The mobility speed is uniformly selected from $[0, v_{\text{max}}]$. Once it is reached a target position, it may pause for a specific amount of time before moving toward the next position which leads to a jagged mobile node distribution in the ad hoc networks. Nevertheless, at the starting of the simulation, 50 nodes are present in the test. It has two series of scenarios based on the mobility model. The first series of scenarios have a fixed $v_{\text{max}}$ but different network densities by varying the network dimensions. The second series have the same network density but varying $v_{\text{max}}$.

5. Results and Discussions

At first study is made at the performance of PSR, and SDFRP in supporting 20 TCP flows in networks with different node densities. Specifically, with the default 250-m transmission range in ns-2, deploy the 50-node network in a square area of varying side lengths that yield node densities of approximately 5, 6, 7 . . . 12 neighbors per node. These nodes move following the random waypoint model with $v_{\text{max}} = 30$ m/s. It plots in Fig. 2 the per-node per-second routing overhead, when they transport a large number of TCP flows. This figure shows that the overhead of SDFRP outperforms PSR. The routing overhead of PSR and SDFRP goes up gradually as the node density increases. This is a typical behavior of proactive routing protocols in MANETs. Fig. 3 plots the TCP throughput of PSR and SDFRP for the same node density levels as before. The total throughput of the 20 TCP flows of SDFRP is noticeably higher than that of PSR. In most cases, SDFRP has the highest throughput because it needs to give up the least network resources for routing.

Next, it focuses on the end-to-end delay of TCP flows to investigate how well these protocols support time-sensitive applications. Fig. 4 shows the delay measured for different node densities and it is obvious that the proposed SDFRP consumes lesser delay than that of PSR. It also studies the performance of SDFRP and compares it to PSR with different rates of node velocity.

In particular, conduct another series of tests in networks of 50 nodes deployed in a $1100 \times 1100$ (m2) square area with $v_{\text{max}}$ set to 0, 4, 8, 12, . . . , 32 (m/s). The network thus has an effective node density of around seven neighbors per node, i.e., a medium density among those configured earlier. As with before, 20 TCP one-way flows are deployed between 40 nodes, and measure the routing overhead, TCP throughput, and end-to-end delay (see Figs. 5–7). The routing overhead of the two protocols (SDFRP and PSR) with varying rates of node velocity is plotted as in Fig. 5. Note that the velocity to the right of the x-axis corresponds to the middle axis in Fig. 2. It is observed in the plot that, as $v_{\text{max}}$ decreases, the overhead of all protocols comes down.

The TCP throughput and end-to-end delay are plotted in Figs. 6 and 7, respectively. From these figures, it is observed that the performance of SDFRP and PSR are similar provided with SDFRP leading the pack in most cases. In addition, neither throughput nor delay is affected by the different rates of velocity. The only exception is that, when $v_{\text{max}} = 0$, both the PSR and SDFRP protocols yield a high throughput of more or less 900 kb/s.

It also tested the protocols for their performance in transporting a small number of UDP streams. Here, it deploys three two-way UDP streams to simulate compressed voice communications. It is to measure and plot the packet delivery ratio PDR (see Fig. 8), delay (see Fig. 9), and delay jitter (see Fig. 10) against varying node densities. In Fig. 8, the PDRs of the two protocols are in the same ball park across different node densities. When the nodes are neither too sparse so that the network connectivity is good nor too dense so that the channel can be spatially reused, these protocols have a fairly high PDR of over 70% for both SDFRP and PSR. On a related note, the delay jitter (see Fig. 10) of SDFRP is significantly lower than that of PSR. Note that voice-over-IP (VoIP) applications usually discard packets that arrive too late. Therefore, the jitter among the packets actually used by the VoIP receiving agent is much smaller. However, the metric still reflects how consistent these protocols are in delivering best-effort packets.
The same measurements are taken to test the two protocols in response to different rates of node velocity. As with the case earlier, it picks three node pairs out of the 50 nodes and gives them two-way constant bit rate (CBR) streams. For the entire series of different velocity caps $v_{\text{max}} = 0, 4, 8, 12 \ldots 32 \text{ m/s}$, the node density is again set to around seven neighbors per node. From the plot of PDR (see Fig. 11), it is observed that PDR of PSR, and SDFRP is always over 70% even when $v_{\text{max}} = 32 \text{ m/s}$. It is noted that the proposed protocol SDFRP is reliable in data delivery when $v_{\text{max}} = 0$ or $4 \text{ m/s}$, where the loss rates are well below 10%. The protocols PSR and SDFRP’s performance in terms of PDR degrades gracefully as the rate of node velocity increases. The end-to-end delay (see Fig. 12) presents a rather distinct landscape. In all cases, the delay for SDFRP is smaller compared with PSR. On the other hand, the measured delay jitter (see Fig. 13) indicates that both PSR and SDFRP protocols become less consistent when nodes move faster. Relatively speaking, however, the variance of SDFRP is much smaller than the other three.
Fig. 7. End-to-end delay in TCP with velocity

Fig. 8. PDR in UDP with density

Fig. 9. End-to-end delay in UDP with density

Fig. 10. End-to-end delay jitter in UDP with density

Fig. 11. PDR in UDP with velocity

Fig. 12. End-to-end delay in UDP with velocity

Fig. 13. End-to-end delay jitter in UDP with velocity
6. Conclusions
This research work aims on network and attack model that takes into account of different valid circumstances in communications (collisions, channel error or mobility) as well as malicious behaviors. It allows inferring how they all may affect the performance of the overall retransmission procedure. Routing overhead, throughput, packet delivery ratio and delay metrics are chosen to conduct performance analysis under the two scenarios namely velocity and density. Simulations are carried out using NS2 and the proposed security strategy performs better.

References