Towards an integration of security and quality of service in IP-based mobile ad hoc networks

DOI:
10.1109/GLOCOM.2011.6133684

Link to publication record in Manchester Research Explorer

Citation for published version (APA):

Published in:

Citing this paper
Please note that where the full-text provided on Manchester Research Explorer is the Author Accepted Manuscript or Proof version this may differ from the final Published version. If citing, it is advised that you check and use the publisher's definitive version.

General rights
Copyright and moral rights for the publications made accessible in the Research Explorer are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

Takedown policy
If you believe that this document breaches copyright please refer to the University of Manchester’s Takedown Procedures [http://man.ac.uk/04Y6Bo] or contact uml.scholarlycommunications@manchester.ac.uk providing relevant details, so we can investigate your claim.
Towards an Integration of Security and Quality of Service in IP-Based Mobile Ad Hoc Networks

Peter J. J. McNerney and Ning Zhang
School of Computer Science, University of Manchester
Oxford Road, Manchester, M13 9PL, UK
{mcnerney, nzhang}@cs.man.ac.uk

Abstract—Security and quality of service (QoS) are two areas of mobile ad hoc network (MANET) research which have so far been largely carried out separately. Some of the unique characteristics of MANETs make them extremely vulnerable to security attacks, and these attacks have a direct impact on QoS provisioning. We therefore argue that integrating security and QoS may be the most effective way of providing QoS in MANETs that contain malicious nodes, and hypothesize that context-aware adaptive multi-path routing may mitigate the damaging effects of denial of availability (DoA) attacks, thus bettering QoS provisioning. As our first step towards validating this hypothesis, this paper investigates whether a single path should be sought using a reservation-based or a non-reservation-based approach.

We compare INSIGNIA, a reservation-based approach to QoS provisioning in MANETs, with Dynamic Source Routing (DSR), a best-effort MANET routing protocol, using simulation. The performance of these two approaches is evaluated in the presence of a variable number of malicious nodes executing blackhole and grayhole data packet forwarding attacks and a denial of QoS attack. The simulation results show that INSIGNIA outperforms DSR when the traffic load is at a medium-to-high level and the threat level is at a low-to-medium level. This performance enhancement brought by INSIGNIA under these particular conditions is because of its single-path adaptation capability. These findings indicate that under certain conditions, e.g., when the network traffic level is low but the threat level is high, the single-path adaptation mechanism is no longer sufficient, and adaptive multi-path routing may help to better QoS support.

Keywords-Mobile ad hoc networks; quality of service; security; availability.

I. INTRODUCTION

A MANET is a collection of autonomous mobile nodes which communicate with one another using wireless links. They cooperate in a distributed fashion to provide necessary network functionality in the absence of any fixed network infrastructure. MANETs are emerging as access networks to the fixed Internet, forming the so-called Internet-based MANETs (IMANETs) [1]. However, MANET characteristics — such as limited node resources, battery power, node mobility, and the provision of routing functionality by network member nodes — open the door to a wide range of general failures and security attacks, both of which can have a profound effect on quality of service (QoS) provision in MANETs and IMANETs.

General failures may lead to the delay or loss of data packets and thus disrupt QoS provision. Examples of such failures include link breakage, resulting from nodes roaming out of wireless range, and battery depletion, which can be attributed to the limited battery life of devices and the expensive nature of wireless communications. In a MANET, where a single device may serve as a router for several nodes’ packet flows, the failure of one device may lead to the disruption of several nodes’ flows and, consequently, a degrading of QoS support.

Security attacks also pose a considerable threat to QoS provisioning. The limited node resources may encourage nodes to be selfish in serving others in order to preserve their own resources. In addition, malicious intent may lead to security attacks which seek to delay or disrupt data packet delivery. These attacks include blackhole, grayhole, and denial of QoS request attacks. The outcome of both security attacks and general failures is that the MANET connections are dynamic and unstable, making QoS provisioning a challenging task.

This paper sets forth our vision for an integrated approach to security and QoS. As the implications of most of the attacks are identical to those caused by failures and mobility it may be more cost effective to integrate the two issues rather than dealing with them separately. This approach may allow us to achieve QoS with reduced costs to nodes’ resources and bandwidth, which, in turn, will bring benefits to QoS provisioning. One way to achieve this integration may be through the use of a context-aware approach to route redundancy.

As our first step towards realizing this vision, this paper investigates the implications of denial of availability (DoA) attacks on two single-path delivery approaches: a best-effort approach using the Dynamic Source Routing (DSR) protocol vs. a reservation-based approach using the INSIGNIA QoS framework. We simulate blackhole and grayhole attacks on DSR and INSIGNIA in addition to a denial of QoS attack on INSIGNIA, and examine the effects of these attacks on packet delivery ratios and throughput, two QoS parameters. Through this simulation we aim to identify QoS effecting attributes under various threat conditions and to investigate which approach, best-effort or reservation-based, performs better and under what conditions. The findings from this study will serve our next stage design, allowing us to exploit an appropriate architecture for context adaptation and an effective QoS approach for context-aware QoS provisioning.

The remainder of this paper is organised as follows. Section II first reviews existing efforts on supporting security and QoS in MANETs and then discusses the need for an integrated approach to security and QoS in this context. Section III first gives the simulation configuration and methodology and
Section IV concludes the paper and outlines our future work. Finally, Section IV concludes the paper and outlines our future work. Then describes and analyses the simulation results. Finally, Section IV concludes the paper and outlines our future work. These out-of-band, i.e., separately from data packets, to inform a process known as QoS reporting. Reports are transmitted of every IP packet. In addition to reducing signalling overhead, encapsulating the signalling information in the IP option field and adaptive in response to dynamic changes in network conditions and topologies. It uses in-band QoS signalling by delivering for high priority traffic and best-effort delivery for lower priority traffic. INSIGNIA is designed to be lightweight resource reservations can tie-up routers’ resources. As this hybrid provisioning can limit the processing and memory resources committed to resource reservations, it provides a novel approach to QoS provisioning in environments where resources are constrained.

INSIGNIA [3] is a QoS framework specifically designed for IP-based MANETs. It supports two levels of QoS: reserved delivery for high priority traffic and best-effort delivery for lower priority traffic. INSIGNIA is designed to be lightweight and adaptive in response to dynamic changes in network conditions and topologies. It uses in-band QoS signalling by encapsulating the signalling information in the IP option field of every IP packet. In addition to reducing signalling overhead, this method also allows INSIGNIA to support the fast restoration and re-routing of reserved data flows during the lifetime of an ongoing session. QoS adaptation is supported through a process known as QoS reporting. Reports are transmitted out-of-band, i.e., separately from data packets, to inform a source node of the success or failure of a reservation. These reports allow source nodes to scale-up or scale-down QoS requirements in response to measured network conditions.

The Hybrid QoS Model for MANETs (HQMM) [4] is inspired by the ideas used in FQMM and incorporates the merits of INSIGNIA. As in FQMM, HQMM provides per-flow QoS to a small proportion of traffic, i.e., high-priority traffic, and per-class QoS to all of the remaining traffic. The per-flow traffic is served using INSIGNIA.

Another category of efforts on supporting QoS in MANETs is by designing QoS routing protocols. These protocols are designed to satisfy some specified QoS requirements by adding relevant QoS parameters into the routing table of each node. When a path is required the corresponding QoS parameter values associated with each path are calculated, and the path with the best value is chosen. The commonly used QoS parameters in early QoS routing protocols, such as QoS-AODV (Quality of Service AODV) and on-demand QoS routing (OQR) [5], are end-to-end delay and bandwidth. Other protocols, e.g., Reliable AODV and AODV Backup Routing [5], are designed to optimize packet delivery reliability in the presence of network dynamics, so they use packet delivery reliability, or loss ratio, as their QoS parameters.

More recently designed MANET QoS routing protocols have started using other additional information, e.g., energy and/or trust, as QoS parameters to make routing decisions energy- and/or trust-aware. The SQ-AODV protocol [6] is an example of an energy-aware QoS routing protocol. It defines a new QoS parameter, called residual node energy, and uses it to govern path selections. It utilizes a cross-layer approach to estimate residual node energy and feeds this estimation into the path selection and maintenance process, thus minimizing connection interruptions due to battery depletion.

Trust-aware (or reputation-based) QoS routing protocols, such as the one proposed in [7], incorporate some security attributes into the route discovery process to ensure that a selected path satisfies a specified security requirement. For example, a node is selected if its trust level is over a specified threshold. If more than one route satisfies the security requirement, the shortest one in the set will be chosen. The main goal of this category of solutions is to estimate the trust levels of neighboring nodes, and based upon the trust levels select the next hop node. A good number of such protocols have been published; they differ on the rating or trust derivation algorithms used (e.g., trust derivation may be based on direct experiences and/or on recommendations by others). These trust-aware routing solutions can, to some extent, mitigate the risks imposed by internal attackers (i.e., attacks imposed by communication participants), and the most notable internal attacks are denial of availability (DoA) attacks.

Most research efforts on addressing security issues at the network layer of MANETs focus on the design of secure routing protocols [8] to counter external attacks, i.e., attacks imposed by external entities. Examples of external attacks are eavesdropping and interception, modification, replay, and fabrication of routing messages. Although external attacks may not directly affect network operations, they are often a
prerequisite for launching more advanced or internal attacks. Cryptographic primitives and techniques, such as encryption, message authentication using keyed hash functions or digital signatures, are used to thwart most of the external attacks.

To date, security and QoS in MANETs have largely been dealt with as two separate issues. Though trust-aware QoS routing protocols have used some security attributes, e.g., trust level, as their underlying QoS parameter to govern path selections, almost all of them (with the exception of the work in [7]) have used the ‘best-effort’ approach, i.e., to select a node that is the most trustworthy, or one with its trust level above a certain threshold, as the routing candidate. The paper [7] tries to integrate security into ad hoc routing by proposing that an application should be allowed to specify the quality-of-protection or some security attributes, and that these security attributes should be taken into account in routing decisions. It describes how routing protocols, such as AODV or DSR, may be extended to carry the values of these security attributes, and how intermediate nodes may access and respond to these attribute values, thus providing the quality-of-protection specified by the application. However, the proposal assumes that the intermediate nodes will conform to the security requirements conveyed in these security attributes, and that they will follow the specifications of the protocol. These assumptions are unrealistic in open MANET environments.

B. Our Idea

It can be seen from the analysis of the existing work that most of the existing MANET QoS solutions focus on achieving a more deterministic network behaviour in the face of resource restrictions and node mobility. The approaches taken by these solutions are largely three: (1) making a hybrid use of the per-flow bandwidth-reserved delivery and per-class best-effort delivery thus improving scalability, (2) supporting end-to-end adaptation in response to fluctuating bandwidth availability, and (3) selecting nodes that are most reliable (most trustworthy and/or with the highest level of residual node energy) to optimize delivery reliability. The adaptation is done by switching between these two delivery services to serve a reserved data flow in response to bandwidth availability. These solutions do not consider the implications of security attacks on QoS. They assume that intermediate nodes always cooperate in performing QoS functions, and that they always faithfully follow the specifications of QoS protocols and mechanisms. Although a trust level, the sole security related attribute used in existing MANET QoS routing protocols, has recently been introduced to govern QoS routing decision making, the decisions made are still a binary one, i.e., ‘yes’ (to select the node/path) or ‘no’ (not to select the node/path). In other words, despite these existing efforts, there are still many open issues to be addressed, e.g., how to support QoS requirements that encompass security requirements? How to best support one’s QoS requirements in presence of malicious attacks? What if intermediate nodes are not co-operating in performing, or even intentionally compromising, QoS functionality, and so on?

A prerequisite for supporting QoS in MANETs is to maximize the probability of successfully delivering a data flow from a source to its intended destination in the presence of network dynamics and malicious attacks. An intuitive way of achieving this is to use route redundancies, i.e., multi-path routing. However, using route redundancy will introduce additional processing and storage overheads at intermediate nodes and will increase network traffic level, both of which will cause adverse effects on QoS provisioning. So route redundancy should only be used when there are no better alternatives to deliver a data flow. To investigate the conditions or context under which the use of a single-path delivery service is no longer sufficient, and/or the use of multi-path routing is essential, the next section presents our preliminary simulation study of two single-path delivery approaches, non-reservation-based (NRB) and reservation-based (RB). The intention here is to investigate which of these two approaches will provide a better data packet forwarding service in malicious network environments.

III. PRELIMINARY STUDY OF NRB VS. RB APPROACHES IN MALICIOUS NETWORK ENVIRONMENTS

This simulation study compares INSIGNIA and DSR in MANETs containing malicious nodes. DSR [9], an exemplary reactive source routing protocol for MANETs, is used as our NRB approach. It treats all data packets with best-effort priority. The INSIGNIA QoS framework, described in Section II-A, is used as our RB approach.

The following four assumptions are made in our study: (i) nodes executing blackhole or grayhole attacks only drop data packets, i.e., they correctly forward DSR control packets and INSIGNIA QoS reports; (ii) we consider all of the obtained network information, such as hop counts, source routes, bandwidth availability, etc., to be a faithful representation of the network; (iii) a node performing a grayhole attack only drops data packets marked to receive reservation-based treatment from INSIGNIA; and (iv) all attacker nodes operate independently, i.e., they do not collude.

The simulation study is conducted using the event driven network simulator NS-2 (version 2.1b3) [10].† We use the CMU Monarch extensions (version 1.1.2) [11] which provide the DSR protocol and several wireless networking enhancements for NS-2. The INSIGNIA source code for NS-2 [12] is used. Nodes move according to a random waypoint model [13]. The 802.11 protocol is used at the MAC layer with a data rate of 2Mbps.‡ When simulating using INSIGNIA, QoS traffic makes up 30% of the constant bit rate traffic with the remaining 70% transmitted with best-effort service. A summary of simulation parameter values is given in Table I.

A variable percentage of network nodes perform blackhole, grayhole, and denial of QoS request attacks on data packets. The blackhole attack is simulated by checking whether a received packet is a data packet and discarding it if so. The

†This older version of NS-2 is used for compatibility with INSIGNIA.
‡A data rate of 2Mbps makes our simulation comparable with the original INSIGNIA research [3].
TABLE I
NETWORK CONFIGURATION AND SIMULATION PARAMETERS.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Network Configuration</strong></td>
<td></td>
</tr>
<tr>
<td>Topology</td>
<td>1000m x 1000m</td>
</tr>
<tr>
<td>Simulation Time</td>
<td>900 s</td>
</tr>
<tr>
<td>Number of Nodes</td>
<td>50</td>
</tr>
<tr>
<td>Node Speed</td>
<td>1–19 m/s</td>
</tr>
<tr>
<td>Mobility Model</td>
<td>Random Waypoint</td>
</tr>
<tr>
<td>Pause Time</td>
<td>0 / 300 / 600 / 900 seconds</td>
</tr>
<tr>
<td><strong>Traffic Model</strong></td>
<td></td>
</tr>
<tr>
<td>Traffic Type</td>
<td>Constant Bit Rate (CBR)</td>
</tr>
<tr>
<td>Number of Sources</td>
<td>10 / 20 / 30</td>
</tr>
<tr>
<td>Packet Size</td>
<td>512 bytes</td>
</tr>
<tr>
<td>Packet Per Second</td>
<td>4</td>
</tr>
<tr>
<td>Ratio of BE to QoS Packets</td>
<td>70:30 (for INSIGNIA traffic)</td>
</tr>
<tr>
<td><strong>MAC Protocol</strong></td>
<td></td>
</tr>
<tr>
<td>Protocol</td>
<td>802.11</td>
</tr>
<tr>
<td>Packet Buffer Size</td>
<td>50</td>
</tr>
<tr>
<td>Nominal Range</td>
<td>250 meters</td>
</tr>
<tr>
<td><strong>Attack Scenarios</strong></td>
<td></td>
</tr>
<tr>
<td>Attack</td>
<td>Blackhole / Grayhole / Denial of QoS Requests</td>
</tr>
<tr>
<td>Attacker Ratio</td>
<td>0%, 10%, 20%, 30%, 40%, 50%</td>
</tr>
</tbody>
</table>

grayhole attack functions similarly, but it only drops data packets receiving QoS treatment from INSIGNIA. The denial of QoS request attack [14] is simulated by checking whether the reservation bit is set in the header of an INSIGNIA data packet and modifying it to best-effort if so. The attacker ratio ranges from 0%, representing a non-malicious network environment, to 50%, in increments of 10%. While 50% of network nodes behaving maliciously may seem artificially high, it provides an opportunity to evaluate the performance of the NRB and the RB approaches in highly adverse and unreliable conditions.

Due to space limitations we only include a small selection of graphs from simulations with a zero second pause time. These are chosen as they provide some of the most interesting results, owing to the challenging conditions arising from the high level of node mobility. The packet delivery ratio (PDR) values for the INSIGNIA reserved traffic (marked as ‘QoS sources’ in the figures) and best-effort traffic (marked as ‘BE sources’) and the DSR traffic are plotted in Fig. 1, with three distinct traffic levels: 10 sources (Fig. 1(a)), 20 sources (Fig. 1(b)), and 30 sources (Fig. 1(c)), respectively. From Fig. 1(a) it can be seen that when the traffic level is light INSIGNIA and DSR perform similarly, with a difference in PDR of < 3%. These PDR values are nearly 100% with a 0% attacker ratio before dropping to approximately 40% when the attacker ratio increases to 20%. From this point the PDR values decrease more gradually and level off at 30% with a 50% attacker ratio.

Fig. 1(b) shows the results when the number of source nodes in the network increases to 20 while all other parameter values remain unchanged. As shown in the figure, when the attacker ratio is 0% the PDR values for the INSIGNIA packets are nearly 70% (a 30% drop compared with Fig. 1(a)), and the value for DSR is about 35% (about a 65% drop). These significant drops at the 0% attacker ratio are due to two factors, both of which are caused by the increased level of traffic in the network. The first factor is that the available network bandwidth is reduced as the network traffic level increases. This is because the increased traffic level means more packet transmissions, and this will lead to more inter-channel interference. As a result there will be more data corruption, leading to further packet drops. The second factor is buffer overflows. With a higher traffic load there will be more packets waiting to be delivered. If the available bandwidth is reduced buffers at the routing nodes will be filled more quickly. Once a buffer is full newly arrived packets will be discarded, causing a higher packet loss ratio.

Another interesting observation on Fig. 1(b) is that, at an attacker ratio of 0%, the PDR value for DSR is much lower than the values for INSIGNIA; the former is only half of the latter. This is because INSIGNIA has an adaptation mechanism...
that allows a destination node to monitor and notify the source node of the reception quality of a data flow. Upon receiving this notification, the source node can either scale-down the QoS requirement or transmit the packets with best-effort forwarding. For example, if packets from a reserved flow arrive as best-effort packets it indicates that the path taken by these packets is running out of spare bandwidth to support the requested reservation, and this means that the path, or this part of the network, is becoming congested. In this case, the destination node will send a QoS Report requesting the source node downgrade QoS packets to best-effort. The general trends of the results in Fig. 1(b) are consistent with the observations in [15], where 20 INSIGNIA sources achieve a higher PDR than DSR in a non-malicious network. It is observed in [15] that network congestion increases at the number of traffic sources increases; the congestion affects DSR more than INSIGNIA. The higher PDR achieved by INSIGNIA is attributed to its service differentiation mechanism and the valuing of high priority flows over best-effort flows. The worse PDR performance exhibited by DSR in our results is due to reduced available network bandwidth caused by channel interference as the result of a higher level of traffic injected into the network.

To explain this observation further we can have a closer look at the DSR results shown in Fig. 1(b). The PDR values of DSR actually increase from 36% to 52% as the attacker ratio increases from 0% to 10%. At a 0% attacker ratio, 91% of the packet loss is caused by overflowing packet queues (due to network congestion). However, when the attacker ratio increases to 10% the PDR is 52%, of which 66% of the packet loss is due to blackhole attacks and 26% is due to overflowing packet queues. In other words, when the traffic level in the network is high and the attacker ratio is small (< 8%) the main cause for packet loss is network congestion, so a small number of blackhole attacks actually serves to reduce the traffic burden in the network. This, in turn, reduces the level of interference, thus resulting in a slight increase in PDR. To validate this finding, we have undertaken a further investigation for a 0–10% attacker ratio in increments of 2%, while keeping all other simulation parameter values the same. The results show a 14% increase in PDR even when the number of blackhole attacker nodes has actually increased from 6% to 8%. The simulation shows that the percentage of packets lost due to blackhole attacks has increased significantly from 10% to 60%. However, the percentage of packets lost due to overflowing downstream packet queues decreases more significantly, thus offsetting the increase in packet loss caused by blackhole attacks.

Fig. 1(c) shows the simulation results when the number of sources is increased to 30. The PDR values for DSR and INSIGNIA fluctuate within the region of 25% to 35% and 30% to 48%, respectively, when the attacker ratio increases from 0% to 50%. As mentioned above, these are the results of the off-setting between two dominant factors of packet losses (network congestion and blackhole attacks).

The second observation from Fig. 1(c) is that the PDR values for INSIGNIA outperform those of DSR by about 20% when the attacker ratio is in the region of 0% to 10%. However, from 10% onward, this gap gradually reduces before the two sets of results join together at the attacker ratio of 30%. As explained for Fig. 1(b), this better PDR value of INSIGNIA is due to its adaptation facility offered by INSIGNIA. However, as the attacker ratio further increases and as blackhole attacks overtake network congestion as the dominant factor for the packet losses, the benefit offered by the INSIGNIA adaptation facility diminishes, causing the two sets of results to converge at a critical attacker ratio (hereafter we call this threshold ratio Attacker Threshold Level, or TL_{Attacker}). This illustrates that at low-to-medium levels of attacker ratios INSIGNIA outperforms DSR. However, when the attacker ratio is high, INSIGNIA’s single-path adaptation facility cannot help to improve the packet delivery ratio. By revisiting Figs. 1(a)–1(c), we can see that TL_{Attacker} increases as the traffic level increases. Obviously, the higher the traffic level, the more blackhole attacks are necessary to offset the packet loss caused by network congestion.

Fig. 2 shows the throughput vs. offered load for INSIGNIA and DSR under the setting of 10%, 30%, and 50% attacker ratios. From these results the following observations can be made. Firstly, there is a threshold of offered load for each attacker ratio setting (we call this threshold value Offered Load Threshold Level, or TL_{OfferedLoad}). Beyond this threshold the network throughput reaches its maximum value and INSIGNIA outperforms DSR, although at the attacker ratio of 50% the benefit brought by INSIGNIA is disappearing. However, before the threshold is reached, INSIGNIA and DSR perform similarly. Another observation is that this threshold value varies with the attacker ratio; the higher the attacker ratio the larger this threshold value. These results show that when the attacker ratio is in the low-to-medium range, INSIGNIA can cope better with heavier network load than DSR in delivering better network throughput values.

Fig. 3 shows the throughput vs. offered load for INSIGNIA under two types of attack: the denial of QoS request (DQoS) attack and the grayhole attack. The same three attacker ratios are used. From the figure, it can be seen that under the DQoS attack the throughputs are generally in an upward trend as offered load increases, regardless of the attacker ratio. This is because the reserved packets are downgraded to best-effort
packets but the packets are still being delivered. In contrast, the throughputs in the presence of grayhole attackers are much lower for nearly all levels of offered load. In the higher end of the offered load, the best achieved throughput value (approx. 150Kbits/s) under the grayhole attack is only half of the best value (330Kbits/s) achieved under the DQoS attack. These results illustrate the necessity for using a redundancy based approach to improve packet delivery ratios under malicious environments.

The above simulation results show that, in terms of throughput and PDR, INSIGNIA generally outperforms DSR. This is attributed to INSIGNIA’s single-path adaptation capability. However, the level of performance enhancements brought by INSIGNIA is dependent on the offered load, i.e., traffic level, and attacker ratios, i.e., threat level, in the underlying network. When the traffic level is in the region of medium-to-high and when the threat level is in the region of zero-to-medium INSIGNIA outperforms DSR markedly. The highest level of enhancement happens when the attacker ratio is zero. When the network is very lightly loaded and/or when the threat level is very high INSIGNIA and DSR perform similarly. This is because, when the network is lightly loaded, the function offered by INSIGNIA’s single-path adaptation facility is not essential to ensure a better level of packet delivery, whereas when the threat level is very high even with the assistance of INSIGNIA’s single-path adaptation facility it is still difficult to improve packet delivery performance. In the latter case, some additional measures are necessary to improve the packet delivery performance. We envisage that context-aware adaptive multi-path routing can be such an additional measure to enhance packet delivery ratios, optimising QoS support in malicious MANETs.

IV. CONCLUSION AND FUTURE WORK

In this paper we have described the need for an integrated support for security and QoS in malicious MANET environments. We have proposed an idea as how such an integration may be realized, i.e., by using an adaptive multi-path routing solution using contextual information to mitigate the damaging effects of DoA attacks. To decide which of the single-path delivery approaches, non-reservation-based or reservation-based, should be used to construct our adaptive multi-path routing solution, this paper has presented our simulation study of these two approaches using the DSR protocol and the INSIGNIA QoS framework under various malicious settings. Through this study we have found that INSIGNIA generally outperforms DSR owing to its built-in single-path adaptation capability, although the level of benefits the former brings over the latter varies with the traffic load and the threat level in the underlying network. These findings point us towards a hybrid use of both single-path and multi-path routing through context-aware adaptation.

As our future work we intend to perform further investigations looking at the performances of the two approaches under different mobility settings before deciding which approach to use in our QoS framework.

REFERENCES