Secure V2V Communications: Performance Impact of Computational Overheads

Aravind Iyer*, Arzad Kherani*, Ashwin Rao† and Aditya Karnik*
*General Motors - India Science Laboratory,
International Technology Park, Bangalore, India
Email: aravind.iyer@gm.com, arzad.kherani@gm.com, aditya.karnik@gm.com
† Indian Institute of Technology - Delhi,
New Delhi, India
Email: ashwin@it.iitd.ac.in

***Abstract*— Safety applications aim to avoid vehicular accidents, by providing advisories to the driver, by using secure broadcast vehicle-to-vehicle (V2V) communications. However, any security mechanism used for authenticating broadcast V2V messages, comes with overheads in terms of computation, storage and communications. Further due to the resource-constrained computing platforms used in the automotive domain, these overheads could translate into performance bottlenecks. Prior works related to performance modeling of secure V2V communications do not consider the computational overheads of security, since traditionally packet transmission rather than packet processing is taken to be the bottleneck. This paper provides an evaluation of the performance of secure V2V communications, while *explicitly* modeling the computational and storage overheads due to security. We observe that there is a complex coupling between the security and the communication layers, and that the performance bottlenecks could shift from one to the other depending on the system parameters. In order to explain these observations, we propose a fixed point based approach which essentially assumes the two layers at a given node independent from each other and from those at other nodes, and uses the inherent consistency relationships to yield fixed point equations for performance metrics such as blocking or collision probability. Our results indicate that this is a promising approach which works quite accurately.**

I. Introduction

Automotive safety applications aim to assist drivers in avoiding vehicular accidents, by providing advisories and early warnings to drivers, using broadcast vehicle-to-vehicle (V2V) communications. Vehicles typically communicate as per the DSRC (Dedicated Short Range Communication) standard [1], and broadcast messages in response to certain random events. V2V communications enable an entire space of applications, in addition to automotive safety, as has been well-documented in [2] and [3]. Since drivers of vehicles participating in V2V communications are expected to act on messages received from other participants, it is clearly necessary that these messages be transmitted in a secure fashion [4], [5].

The problem of authentication of broadcast messages in an ad hoc network setting, has been investigated in some detail in the literature (see [6] and references therein). However, none of the proposed protocols for broadcast authentication are completely satisfactory. According to [6], any protocol for broadcast authentication in ad hoc networks can satisfy at most six of the "seven cardinal properties" identified therein. In particular, digital signatures based on asymmetric key cryptography result in high *computational* overhead, while one-time signatures such as Merkle-Winternitz signatures [7], [8], result in high *communication* overhead, and light-weight protocols such as TESLA [9], result in *delayed message authentication*. This could lead to performance bottlenecks if there are resource constraints on either the computational, communication, or storage capabilities.

Now, computational platforms used in the automotive domain have different design priorities as compared to general-purpose ones. Being highly sensitive to operating conditions, reliability and cost, typical automotive processors operate at lower clock speeds and have limited on-board memory and storage, in comparison to general purpose ones. In addition, applications based on V2V communications, would have to compete with other concurrent applications running on the same automotive processor. Thus, due to limited computational and storage capabilities, and owing to the limited throughput of random access broadcast communications, secure V2V communications are bound to face performance bottlenecks, regardless of the broadcast authentication mechanism used.

The classical view in the communication networking literature is that computational tasks are not resource-constrained, in comparison to communication, and therefore bottlenecks and queuing due to computational overheads are seldom explicitly modeled. Related works in the V2V communication literature such as [10], [11] and [12] attempt to evaluate and improve the performance of vehicular communications, but their work does not explicitly model the computational overheads due to security. Hubaux *et al.* in [4] provide the processing delays associated with the security operations. These delays could be of the order of about 10 ms. In comparison to packet transmission times which are expected to be of the order of several hundreds of μs, these processing delays are clearly not negligible. However, prior works related to performance modeling of secure V2V communications do not consider the computational overheads of security, since traditionally packet transmission is considered the bottleneck.

We evaluate the performance of secure vehicular communication with *explicit* models for processing delays due to

978-1-4244-2219-7/08/$25.00 (c)2008 IEEE

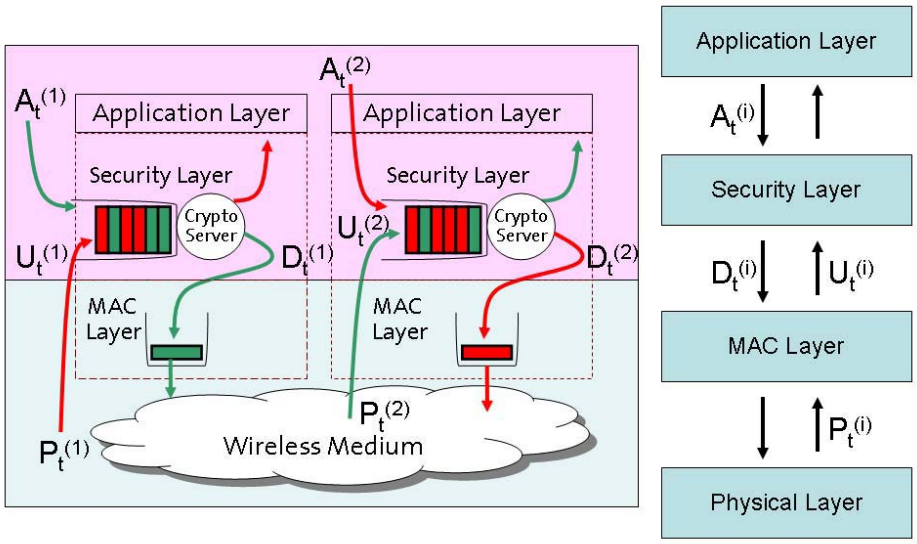

Fig. 1. System Mode: Internals of a V2V-equipped node.

security related operations. We observe that there is a complex coupling between the security and the communication layers, and that the "performance bottlenecks" could shift from one to the other depending on the system parameters. In order to explain these observations, we use a fixed point based approach which is similar in spirit to the one employed in the IEEE 802.11 literature, *à la* Bianchi [13]. The essence of our approach is that we assume that each node sees the environment as an independent averaged-out process, and that the environment is then composed of a large number of such nodes. From the inherent consistency relationships, we derive fixed point equations which capture the behavior of the system. Our results indicate that this is a promising approach which works quite accurately.

In what follows, Section II presents on overview of how we model the internals of a node participating in secure V2V communications, and some simulation results which indicate that either security or communication layers could be the bottleneck. Section III provides an overview of our fixed point based approach to analyze the performance of the system. Section IV compares the numerical and simulation results to show the accuracy of our approach. Finally, Section V concludes the paper.

II. Securing Vehicular Networks: Preliminary Observations

In this section, we present our system model of the internals of a node participating in secure V2V communications, followed by some simulation results which indicate that security processing can also be a "bottleneck". We assume that security (specifically, broadcast authentication) is provided by means of a combination of a PKI (Public Key Infrastructure) and computationally lightweight signatures such as TESLA [9] or Merkle-Winternitz one-time signatures [7], [8]. Under such a framework, nodes could either use digital signatures based on asymmetric key cryptography, using certificates issued by the Certifying Authority (CA) of the PKI, or computationally lightweight signatures mentioned above which use digitally signed messages for conveying a commitment to the lightweight authentication scheme (in particular, "anchor messages" in TESLA or "verifiers" in the Merkle-Winternitz one-time signature scheme - for details, please refer to [9], [7], [8]).

Now we introduce the system model. Each node participating in secure V2V communications, can be thought of as being composed of a stack of layers in the following order.

1. Application Layer: The application layer at a given node generates packets randomly over time, at some (possibly node dependent) rate. The packet generation process could be triggered by occurrence of some random events such as a hazard on the road, or sudden change in speed. For the purpose of this work, we assume that packets are generated by the application layer according to a Poisson process. The mean inter-arrival time is denoted by t_p. The arrival process itself is denoted by $A_t^{(i)}$ which is taken to represent the arrival time of the 't'th packet arriving at node i. The payload of the packets is expected to carry some useful information about the random event that caused the generation of the packet. This information would be used in an appropriate fashion by the application layer of the receiving nodes. In this paper, we do not concern ourselves with the actual payload content of packets.

2. Security Processing Layer: The security layer is responsible for providing broadcast authentication. This is accomplished by two functions: (i) appending the signature of the given node to the packets received from the Application layer ($A_t^{(i)}$), before forwarding them to the communication layers; and (ii) verifying the signatures of the packets from other nodes, as and when passed up by the communication layers. Here, we use $U_t^{(i)}$ to denote the arrival time of the

't'th packet arriving at node i from any of the other nodes. The cryptographic operations described above usually take a random amount of time due to the following factors.

1) In the simple case, when a PKI has only one level of hierarchy (*i.e.,* all the nodes are "under" a single CA), verification of a packet via digital signatures involves verification of the sending node's certificate followed by verification of the sending node's signature. For nodes whose certificate has been authenticated, the first step is optional. However, depending on the hierarchical structure of the PKI tree being used (*i.e.,* number of CA's and hierarchical levels), and depending on how nodes are related to one another in the PKI tree, authenticating a digital signature could involve a random number of certificate/signature verifications.
2) Since V2V applications have to compete with other aplications for a share of processor resources, the latency of completion of cryptographic operations could be random. This is a function of the scheduling policies at the processor, but the latencies in general would be random.
3) Owing to the use of lightweight signatures as well as digital signatures, there would be a considerable variation in the time taken for signature generation and verification, depending on the means used to sign and/or verify the packets. Lightweight signature schemes could be upto 2 orders of magnitude faster than asymmetric cryptography based digital signatures.

The time spent at the cryptographic server is thus a random quantity. We assume it is exponentially distributed with a mean of t_s. The queuing policy at the security server is FIFO (first-in-first-out) as shown in Figure 1. Since V2V nodes are likely to be resource-constrained, the security layer is assumed to have a finite buffer denoted by B in terms of number of packets it can store.

3. MAC Layer: The medium access control (MAC) layer is responsible for packet transmission over the air. The MAC layer transmits the packets generated by the application layer, after they have been signed by the security layer. We index packets by the order in which they are signed by the security layer. We denote by $D_t^{(i)}$ the time the 't'th packet is signed by the security layer of node i. This is the input process to the MAC layer. The MAC protocol used is similar to the random access MAC of IEEE 802.11. However, since V2V packets are broadcast packets, acknowledgments and retransmissions are not employed. Further, retransmissions in such a setting may not be appropriate because of the latency requirements and since newer information is better than the older. Thus, each packet arriving at MAC layer is attempted to be transmitted exactly once. This is in accordance with the DSRC standard [1]. The MAC queuing policy is also FIFO. The random access DSRC MAC layer is modeled using a slotted time system. Thereby, time is assumed to be slotted, and in every slot, we assume that a node that has a packet to transmit, attempts a packet transmission with a probability p. The length of the slot is taken to be equal to the transmission time of a packet (see next).

4. Physical Layer: For the purposes of this work, we use the *single-cell* model for the physical wireless channel. A set of wireless nodes is said to belong to a single-cell if each node can hear every other node, and provided packet transmissions are successful only if exactly one node attempts a transmission. The single-cell assumption results in a uniform impact of the wireless medium on all the nodes present in the system, and makes the system easier to understand. An extension to a node-dependent physical layer is in progress. Packet transmissions are taken to last for a fixed amount of time, denoted by Δ. Evidently, Δ depends on the channel data-rate, and the size of the payload. We account for all these in terms of the single parameter Δ. Packets that are successfully transmitted on the air are indexed by the order in which they complete transmission. We then denote by $P_t^{(i)}$ the time at which the 't'th packet not transmitted by node i, completed transmission. Note that $P_t^{(i)}$ is the same as $U_t^{(i)}$.

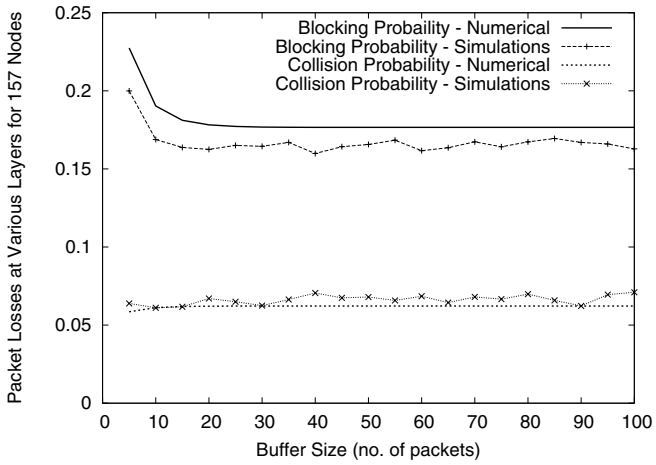

Fig. 2. Packets Lost at Various Layers vs Buffer Size (Scenario 2)

We now present a couple of plots from our numerical and simulation results. The simulation results have been obtained using a slotted-time simulator we developed. The simulator models in detail, all the features of the various layers described above. The numerical results have been obtained from our analytical model which is described in the next section. For now, we depict the percentage of packets lost at the security layer due to blocking, and at the MAC layer due to collisions, as a function of the buffer size. Figure 2 depicts the packet losses for a network of 157 nodes, with t_p=1000 ms, t_s=10 ms and Δ=500 μs (we call these settings of t_p, t_s and Δ as Scenario 2). A packet transmission time of 500 μs corresponds to a 375 byte packet transmitted at 6 Mbps (the data-rate for DSRC). Scenario 2 represents a relatively heavyweight mechanism at use at the security layer, a relatively low frequency of random events which trigger packet generation at the application layer. From the two figures, it can be observed

978-1-4244-2219-7/08/$25.00 (c)2008 IEEE

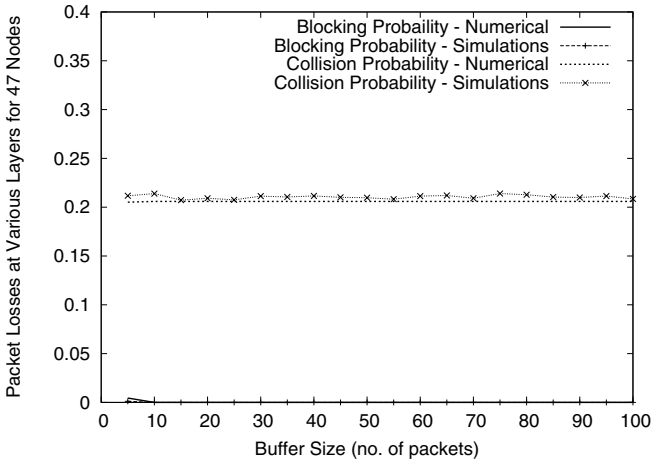

Fig. 3. Packets Lost at Various Layers vs Buffer Size (Scenario 3)

that in Scenario 2, most of the packet losses take place at the security layer Scenario 2 shows that the security layer can also be a bottleneck.

Figure 3 depicts the packet losses for a 47 node network, with t_p=100 ms, t_s=1 ms and Δ=500 μs (we call these settings Scenario 3). Scenario 3 represents a relatively lightweight mechanism at use at the security layer, and a relatively high frequency of packet generation at the application layer. In scenario 3, the packet losses mostly take place at the MAC layer. Scenario 3 represents the more conventional sort of behavior where processing (although it is actualy slower than packet transmission) is not a bottleneck. It may also be noted that the simulation and numerical results are remarkably close.

III. The Fixed Point Approach

The model for the V2V node (see Figure 1) and the simulation results presented in the previous section indicate two salient observations: (i) there is a tight coupling between the security and communication layers both at a given node, and across different nodes because packets from a given node's neighbors also consume queuing resources at the same security queue which serves the given node's packets; and (ii) the performance "bottleneck" could shift from one layer to another depending on the relative time-scales dictated by t_p, t_s and Δ.

Motivated by these two observations, we propose a fixed point based approach to analyse the system, and characterize its performance. The approach that we propose is to essentially ignore the correlations between the processes at different layers at a given node, and across nodes, thus breaking the system down into many *independent* blocks, each of which can be analyzed separately. This is actually along the lines of the standard modeling literature on IEEE 802.11 (see [13], [14]). Specifically, the various processes associated with the different nodes, as introduced in Section II (see Figure 1) are in general, correlated with one another, and possibly also across time. For example, the process $\{D_t^{(i)}\}$ is correlated with the process $\{A_t^{(i)}\}$ and possibly with $\{U_t^{(j)}\}$ for another node j. We ignore these correlations.

Let us denote the total number of nodes in the single cell as N. As mentioned earlier, the arrival process $A_t^{(i)}$ for each node i is assumed to be a Poisson process with a packet generation rate of $\frac{1}{t_p}$. In addition, we assume that the process $U_t^{(i)}$ for each ndoe i is an independent Poisson process with a rate denoted by Λ. Since the service distribution has been assumed to be exponential with rate $\frac{1}{t_s}$, the security queue is essentially an M/M/1 queuing system with a finite buffer B. Therefore, the blocking probability at the security layer buffer, denoted by P_B is given by

$$P_B = \frac{(1-\theta)\theta^B}{1-\theta^{B+1}} \tag{1}$$

$$\text{where } \theta = \frac{\Lambda + \frac{1}{t_p}}{\frac{1}{t_s}} \tag{2}$$

Now owing to the phenomenon of blocking at the security layer, the rate at which packets enter the MAC layer to be transmitted over the wireless medium, is just $\frac{1}{t_p}(1-P_B)$. We assume that the process $D_t^{(i)}$ for every node i is also a Poisson process with rate $\frac{1}{t_p}(1-P_B)$. We model the physical layer as a single cell, and we model the MAC layer attempt process using a slotted time model. Each slot is taken to last Δ time units. In each slot, every node that has a packet attempts a packet transmission with a probability p independently of prior transmissions. Thus, the MAC layer is also an M/M/1 queuing system. Therefore, the probability that a node i has a packet in any given slot is given by

$$\Pi = \frac{\frac{1}{t_p}(1-P_B)\Delta}{p} \tag{3}$$

Now with N nodes in the single cell, the probability that there would be a collision is just the probability of more than one node having a packet and attempting a transmission. Thus, the probability of collision (denoted by P_C) is given by:

$$P_C = 1 - (1-\Pi p)^{N-1} \tag{4}$$

Thus, the application generated traffic from each node gets thinned by a factor $(1-P_B)$ due to blocking at the security layer, and by a further factor $(1-P_C)$ due to packet collisions at the MAC/Physical layer before being received by all the other nodes. As we mentioned earlier, we assume that the process $U_t^{(i)}$ (which is the same as $P_t^{(i)}$) is a Poisson process independent of the application generated packets with a rate Λ. By the above argument, the process $P_t^{(i)}$ (or $U_t^{(i)}$) for any node i would have a rate Λ given by:

$$\Lambda = (N-1)(1-P_B)(1-P_C)\frac{1}{t_p} \tag{5}$$

Now, equations (1), (2), (3), (4) and (5) taken together express the blocking probability P_B in terms of itself, and the collision probability P_C in terms of the blocking probability P_B. We need to prove that the set of equations (1), (2), (3), (4) and (5) form a consistent set of equations and have a solution for P_B using a fixed point equation. This is our immediate research

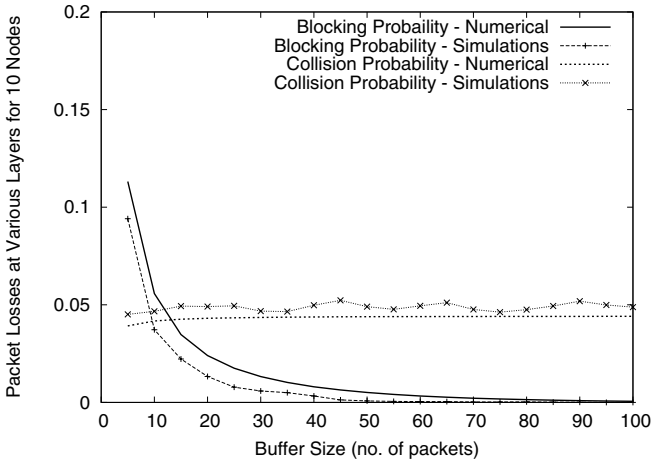

Fig. 4. Packets Lost at Various Layers vs Buffer Size (Scenario 1)

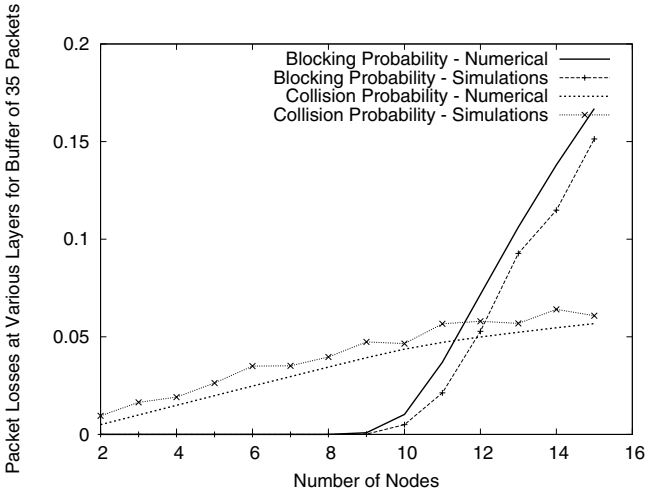

Fig. 5. Packets Lost at Various Layers vs Number of Nodes (Scenario 1)

effort. However, for the scenarios considered in the paper, we do have uniqueness of solution of the above set of equations. Note that the end-to-end throughput of packets from any given node to any other node, is given by

$$\lambda_{e2e} = \frac{1}{t_p}(1 - P_B)^2(1 - P_C) \tag{6}$$

where the subscript $e2e$ refers to "end-to-end". Next we take a look at some more numerical and simulation results.

IV. Numerical and Simulation Results

The simulation results were obtained using a slotted time simulator we developed. The simulations fully model all the features of the various protocol layers as described earlier (see Figure 1). The numerical results were obtained by numerically solving the fixed point equations for the metrics of blocking probability at the security layer, and packet collisions at the MAC layer. The fixed point equations were obtained by assuming statistical independence across layers at a node and across nodes, and the inherent consistency relationships between the layers (*i.e.,* by solving equations (1), (2), (3), (4) and (5)).

Figures 4 and 5 depict the packets lost due to blocking at the security layer, and due to collisions at the MAC layer for Scenario 1 (t_p = 100 ms; t_s = 10 ms; Δ = 500 μs). Scenario 1 is a combination of frequent packet generation and a heavyweight security layer. Thus, it is expected that the security layer could be a bottleneck, and that the system may not scale to a very large number of nodes. These expectations are borne out by the simulation and numerical results. Figure 4 indicates that for a 10 node network, the MAC layer causes only about 5% packet loss, while the blocking at the security layer could be mitigated considerably with increasing buffer size. However, the reduction in blocking probability is insignificant beyond a buffer size B of 35 packets. Figure 5 indicates that for a fixed buffer size of 35 packets, the security layer becomes a bottleneck for more than 10 nodes in the sytem.

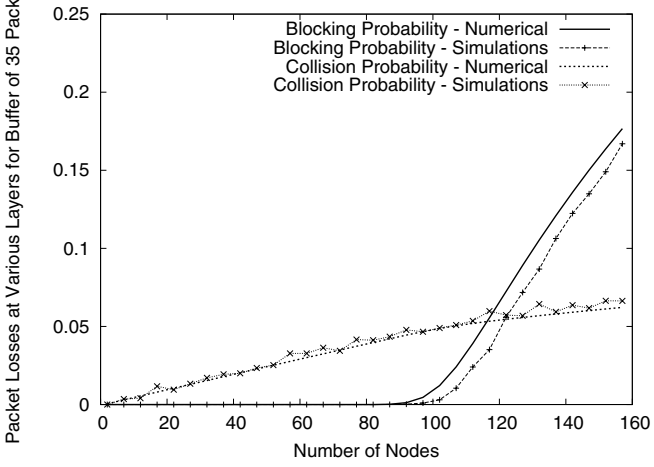

Fig. 6. Packets Lost at Various Layers vs Number of Nodes (Scenario 2)

Figures 6 and 7 depict packet losses for Scenario 2 and Scenario 3, as a function of number of nodes, for a fixed buffer of 35 packets. Scenario 2 shows pretty much the same behavior as Scenario 1, however with the security layer becoming a bottleneck at about 100 nodes, as opposed to 10 nodes as in the case of Scenario 1. Note that in Scenario 1, $\frac{t_p}{t_s}$ is 10, and in Scenario 2, it is 100. However, although $\frac{t_p}{t_s}$ is equal to 100 in Scenario 3 as well, the bottleneck never shifts to the security layer. In fact, the MAC layer is a fairly severe bottleneck resulting in about 20% packet loss for just 50 nodes. Thus, the end-to-end throughput in Scenario 3 is about 20% less than the packet generation rate (see equation (6)). Note that in Scenario 1, the number of nodes for which the end-to-end packet loss is about 20% can be calculated to be about 12 using the date in Figure 5 and equation (6). Thus, from Scenario 1 to Scenario 3, a 10-fold decrease in the computational overhead due to security is actually resulting in about only a 4-fold increase in the number of nodes that can be supported with the same end-to-end throughput.

These results demonstrate a number of things. Firstly,

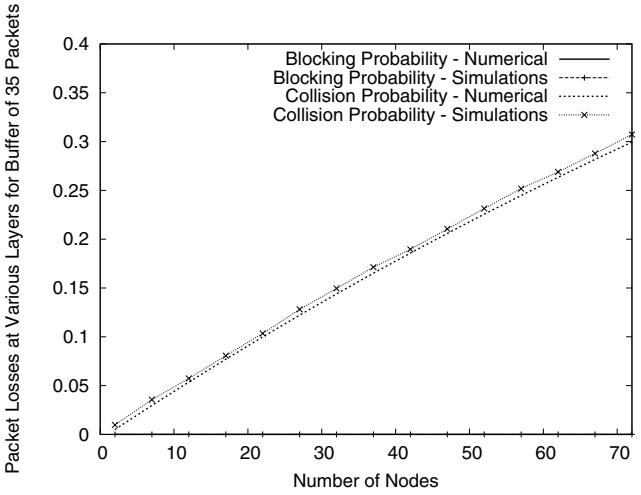

Fig. 7. Packets Lost at Various Layers vs Number of Nodes (Scenario 3)

depending on the relative values of t_p, t_s, Δ and N, the bottlenecks on performance could shift from one of the MAC and security layers, to the other. Secondly, reduction in the average processing times of packets need not result in a proportionate increase in the number of nodes that can be supported by the V2V system. Finally, our analytical model is able to capture all these phenomena with fairly good accuracy, as can be seen from all the graphs.

V. Conclusions and Future Work

Security mechanisms come with overheads that affect the performance of the V2V communications, and hence that of the safety applications. Prior works related to performance modeling of secure V2V communications do not consider the computational overheads of security. Our contributions are two-fold:

- C1 We provide an evaluation of the performance of secure V2V communications, while *explicitly* modeling the computational overheads due to security. We observe that there is a complex coupling between the security and the communication layers, and that the performance bottlenecks could shift from one to the other depending on the system parameters.
- C2 In order to explain these observations, we propose a fixed point based approach. Despite the tight coupling inherent in the sytem, we are able to explain the observations, and our numerical results match quite closely with simulations.

Our immediate research effort is geared towards finding conditions under which the fixed point equation for blocking probability has a solution. This work also offers several avenues for extension in the future, including analysis for a node dependent physical layer, non-Poisson distributed processes for arrival and security processing, and so on.

References

[1] *Standard Specification for Telecommunications and Information Exchange Between Roadside and Vehicle Systems - 5 GHz Band Dedicated Short Range Communications (DSRC) Medium Access Control (MAC) and Physical Layer (PHY) Specifications*, ASTM Std. E2213-03, 2003.

[2] National Highway Traffic Safety Administration, "Vehicle safety communication project - Final Report," U.S. Department of Transportation, Tech. Rep., 2006.

[3] F. Bai, H. Krishnan, V. Sadekar, G. Holland, and T. ElBatt, "Towards characterizing and classifying communinication-based automotive applications from a wireless networking perspective," in *1st IEEE Workshop on Automotive Networking and Applications (AutoNet2006)*, 2006.

[4] M. Raya and J.-P. Hubaux, "The security of vehicular ad hoc networks," in *SASN '05: Proceedings of the 3rd ACM workshop on Security of ad hoc and sensor networks*. New York, NY, USA: ACM Press, 2005.

[5] *Wireless Access in Vehicular Environments - Security Services for Applications and Management Messages*, IEEE Std. 1609.2, 2006.

[6] M. Luk, A. Perrig, and B. Whillock, "Seven cardinal properties of sensor network broadcast authentication," *Fourth ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN 2006), Alexandria, Virginia,*, October 2006.

[7] R. Merkle, "A digital signature based on a conventional encryption function," *Advances in Cryptology - CRYPTO '87*, pp. 369–378, 1988.

[8] ——, "A certified digital signature," *Advances in Cryptology - CRYPTO '89*, pp. 218–238, 1990.

[9] A. Perrig, R. Canetti, J. D. Tygar, and D. Song, "The tesla broadcast authentication protocol," *RSA CryptoBytes*, vol. 5, no. Summer, 2002.

[10] Q. Xu, T. Mak, J. Ko, and R. Sengupta, "Vehicle-to-vehicle safety messaging in dsrc," in *VANET '04: Proceedings of the 1st ACM international workshop on Vehicular ad hoc networks*. New York, NY, USA: ACM Press, 2004, pp. 19–28.

[11] T. ElBatt, S. K. Goel, G. Holland, H. Krishnan, and J. Parikh, "Cooperative collision warning using dedicated short range wireless communications," in *VANET '06: Proceedings of the 3rd international workshop on Vehicular ad hoc networks*. ACM Press, 2006, pp. 1–9.

[12] M. Torrent-Moreno, D. Jiang, and H. Hartenstein, "Broadcast reception rates and effects of priority access in 802.11-based vehicular ad-hoc networks," in *VANET '04: Proceedings of the 1st ACM international workshop on Vehicular ad hoc networks*. ACM Press, 2004.

[13] G. Bianchi, "Performance analysis of the ieee 802.11 distributed coordination function," *IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS*, vol. 18, no. 3, pp. 535–547, March 2000.

[14] A. Kumar, E. Altman, D. Miorandi, and M. Goyal, "New insights from a fixed point analysis of single cell ieee 802.11 wlans," in *Proceedings of IEEE Infocom'05*, 2005.

978-1-4244-2219-7/08/$25.00 (c)2008 IEEE