International Journal of Engineering & Technology, 7 (4.6) (2018) 354-357

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Differentiation of Natural and Maliciously Induced Packet Loss in Wireless Network Using Forensic Analysis

Karthikeyan N[1], Godwin Ponsam J[2]

[1,2] *Department of Information Technology,SRMI nstitute of Scienceand Technology,*
**Corresponding author E-mail: Karthikeyan_n17@srmuniv.edu.in*

Abstract

Wireless networks are prone to packet loss making it strenuous to differentiate if data leakage is due to the physical nature of wireless networks or from malicious packet loss.All previous experiments were made on utilizing nodes which are part of network to monitor packet loss , a method deployed in passive detection.Due to high levels of interference the likelihood of classifying malicious packet loss from wireless induced packet loss is less probable.In this paper using certain transmission parameters like traffic intensity ,node density and transmission evidence we perform forensic analysis. By using an analytical framework we compute the transmission evidence.We validate our analytical framework via both simulation and wireless test-beds.The analytical framework is then used as a basis for a protocol within a forensic analyser to assess the cause of packet loss and determining the likelihood of forwarding misbehaviours.

Keywords: *Forensic analysis,malicious intent,transmisssion evidence,packet loss*

1. Introduction

Wireless networks are applicable in various important area such as disaster recovery.Packet forwarding is the integral part of the wireless networks.Various studies regarding the packet loss are performed in which malicious routers do not allow in packet transmission. The characteristic of the wireless networks is such that it is very strenuous to differentiate packet loss due to the inherent nature of the wireless networks from the packetloss due to the malicious intruders.Forensic analysis helps us in evaluating packetloss,but the existing systems fail to differentiate the packetloss due to the induced effect from the packetloss due to the malicious intent.Generally existing system evaluate packetloss using nodes part of network.However we cannot deploy nodes at huge scale,which it requires to monitor the malicious drops.Since we cannot deploy many nodes the likelihood of detecting malicious drops become difficult. In this project ,we evaluate what is the likelihood of detecting malicious drops using physical parameters such as the traffic per unit volume and network per unit volume.We evaluate how to differentiate malicious drops from inducedloss.

In regard with the above requirements we construct an analytical framework which uses physical parameters of the network as the input.This provides us with the evidence regarding the transmission.This is
called "Transmission evidence".It is also called as TE.The analytical network is the basis of forensic analyser.

1) Transmission evidence depends on node availability,packet size,bit rate,network traffic and is checked end to end and on the linkbasis.

2) Analysis using framework viaboth the simulation and real environment.We perform extensive simulation using both analytical framework and also using test bed.

3) **Forensic analysis:**Our analyser computes the likelihood of transmitter and receiver disregarding packets.It takes as input a)network parameters and b)logs on the network.It then yields whether the transmitter or receiver as disregarded thepacket.

4) **Scope of the work:**Our analytical framework performs coarse grained analysis and extensive analysis.Coarse grained method of analysis uses only static method.Only single packet is considered.While performing extensive analysis a wide range of network parameters and dynamic method.This method of analysis is heterogeneous.More advanced method could be employed in the future to minimize the variation from the actualvalue

5) **Likelihood of detection:**The more the drops of the attacker the more we can conclude that the malicious intent is involved and the more the likelihood of detection.

2. Related Work

Related literature on forensics of the network and the characteristic of the packet loss in wireless networks isstudied.

A previous work on wireless monitoring at the *mechanism and system design* , a scheme to identify nodes which are malicious and behave abnormally with packet forwarding along a multi hop path. Another model deals with design and implement flux; flux automates forensics and identifies traffic vulnerabilities and network threats.

Some of the previous papers provide metric for calculating the packet loss but do not identify the packet loss due to wireless networks.Other papers calculate the packet loss using the collision detection,interference and fading techniques.None of the above methods differentiate packet loss due to the malicious intent. The paper which is close to this paper is J.ning ,but it uses coarse grained technique where a static method is used ,but we consider both static method and dynamic method where a heterogeneous

method is used instead of homogeneous method ,a wide range of network parameters are considered.

3. Framework for Analysis

A framework is developed such that it calculates the transmission evidence.We consider that the sender and the receiver do deny the packets.We are applying the forensic analyser in the framework
Collection of evidence:
(i)The sender stores the evidence in the form of acknowledgement packets.
(ii)The receiver also stores the packets and is locally verified.
(iii)A node is also deployed additionally and it acts as the evidence aware node.
(iv)The overhead due to the evidence collection is neglected.
(v)Overhead due to the digital verification is analysed and is negligible.
(vi)Overhead due to the acknowledgement packets is also negligible.

N	Total number of nodes
v_i	Transmitter
v_j	Receiver
d_{v_i,v_j}	Distance between v_i and v_j
P_{v_i,v_j}	Received power at v_j from v_i
h_{v_i,v_j}	Channel attenuation between v_j and v_i
η	Expected value of $\lvert h_{v_i,v_j}\rvert^2$
P_t	Transmission power
P_n	Noise power
α	Path loss exponent
z	Number of interferers
Z	Set of interferers
λ	Expected traffic sent per node in unit time
Λ	Expected interference level perceived by a node projected from another node in unit time
r	Transmission bit-rate
γ	SINR threshold
l_D	data packet length
l_A	ACK packet length

TABLE I: Notations

Evidence source 1: Transmitter gets the acknowledgement packet from receiver

$$Pr_{src1} = Pr\left(succ \mid r, l_D\right) \cdot Pr\left(succ \mid r_0, l_A\right). \quad (1)$$

Evidence source 2:The Receiver has a evidence which is stored.

$$Pr_{src2} = Pr\left(succ \mid r, l_D\right). \quad (2)$$

$$Pr_{src3\_D} = \sum_{z=0}^{N-2} Pr\left(\mathrm{z}\ \ int \mid r, l_D\right) \cdot \left(1 - \left(1 - Pr\left(succ \mid r, l_D, z\right)\right)^{N-z-2}\right), \quad (3)$$

Evidence source 3: This is another extra node which is deployed and acts as a witness

$$Pr_{src3\_A} = Pr\left(succ \mid r, l_D\right) \cdot \left(\sum_{z=0}^{N-2} Pr\left(\mathrm{z}\ \ int \mid r_0, l_A\right) \cdot \left(1 - \left(1 - Pr\left(succ \mid r_0, l_A, z\right)\right)^{N-z-2}\right)\right). \quad (4)$$

$$Pr_{src3} = Pr_{src3\_D} + \left(1 - Pr_{src3\_D}\right) \cdot Pr_{src3\_A}. \quad (5)$$

HTE AVAILABILITY:

Here we assume that the witness is not dependent

$$Pr_{HTE} = 1 - \prod_{i=1}^{3} Pr(source\ i\ is\ unavailable) = 1 - (1 - Pr_{src1}) \cdot (1 - Pr_{src2}) \cdot (1 - Pr_{src3}). \quad (6)$$

Retransmission of data: Retransmission depends whether the previous data packets are transmitted successfully or not.The success of the previous data transmission determines whether the packet is to be transmitted or not.

$$Pr_{succ\_ex} = Pr\left(succ \mid r, l_D\right) \cdot Pr\left(succ \mid r_0, l_A\right), \quad (7)$$

If there are i transmissions then the If the limit is n_r

$$Pr_{HTE}[n_r] = \sum_{i=0}^{n_r} Pr(rtx = i) \cdot \left(1 - (1 - Pr_{HTE})^{i+1}\right). \quad (8)$$

Transmission evidence at the path level: Path level transmission evidence is the witness related form the start to the end.We consider the PTE is independent for different paths or hops ,but it is not independent.Here the effects are negligible.Our experiments deems it acceptable.PTE means that all the hop level transmission evidence is considered and is denoted by

$$Pr_{PTE}[H] = \prod_{h=1}^{H} Pr_{HTE}[at\ h^{th}\ hop]. \quad (9)$$

Selection of Bit-rate: Variation of bit rates leads to variation in the transmission evidence.It depends on the fluctuations due to the distance and fading.We cannot obtain different distribution rates for different rates.We just a select a random bit rate.But we can incorporate all the bit rates in the analysis section.We can also analyse various distribution obtained due to this.The Path transmission evidence availability depends on the hop level transmission evidence availability.

$$P_{v_i,v_j} = \frac{P_t \cdot \lvert h_{v_i,v_j}\rvert^2}{d^{\alpha}_{v_i,v_j}}, \quad (10)$$

Case	TE availability probability
Transmitter lying	0
Transmitter not lying, receiver receiving the packet and not lying	1
Transmitter not lying, receiver receiving the packet and lying	Pr_{src3_D}
Transmitter not lying, receiver not receiving the packet	Pr_{src3_D}

TABLE II: TE availability under all possible cases

4. Calculating the Availability:

Here the commonly used network parameters are considered such as the traffic,packers per unit volume of the nodes.
The signal power from sender to receiver is given by
The SINR model:SINR model is Signal to interference and Noise and is given by

$$\frac{P_{v_i,v_j}}{P_n + \sum_{k \in \{1,\ldots,N\} \setminus \{i,j\}} P_{v_k,v_j}} > \gamma, \quad (11)$$

Instead of using the Media access control to a specific scheme ,we use the interference scheme.
Node distribution is uniform.
We compute TE availability using the parameters of the transmitter and receiver,we also consider interference ,fading and the equation is given by

$$Pr\left(succ \mid r, l_D, d_{v_i,v_j}, z\right) = Pr\left(\frac{P_{v_i,v_j}}{P_n + \sum_{k \in Z} P_{v_k,v_j}} > \gamma\right), \quad (12)$$

The model depends on both the traffic per unit volume and media access control.If the fading is due to the time division Multiple access model then the interference is low,if it is based on the ALOHA model then the interference is high.
If we are to consider the uniform node it is given by
(1…….N)

$$Pr\left(succ \mid r, l_D\right) = \int_0^R Pr\left(succ \mid r, l_D, d_{v_i,v_j}\right) \frac{2d}{R^2} dd. \quad (13)$$

5. Forensic Analytic Framework

The analytic framework is used along with the forensic analyser.Utilizing the framework we compute the probabilities of obtaining transmission evidence offline using the physical parameters.We then compare these values with what is actually performed on the network ,we also consider about the sender and receiver denying in the false manner.If the packet loss is due to the malicious packet then the value will be slightly exaggerated from the offline computed value.The more intent the aggressor hasthe more the likelihood of variation from the projected values to the actual value.
Analysis using forensic analyser:The forensic analysis is performed based on the two evidences:(i) the offline computed probabilities (ii)The witness evidence collected practically.

The below diagram explains the forensic analyser.

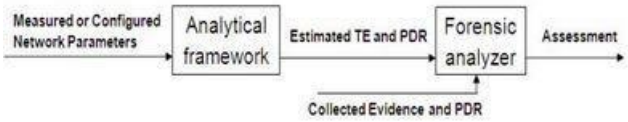


Fig. 1: Forensic analyzer

Analysing misbehaviours: We consider all the nodes from the start to the end.We consider both the sender and receiver denying falsely.

$$Pr_{HTE} = 0 \cdot Pr[transmitter\ lying] + 1 \cdot (1 - Pr[transmitter\ lying]) \cdot Pr_{succ} \cdot (1 - Pr[receiver\ lying]) + Pr_{src3\_D} \cdot (1 - Pr[transmitter\ lying]) \cdot Pr_{succ} \cdot Pr[receiver\ lying] + Pr_{src3\_D} \cdot (1 - Pr[transmitter\ lying]) \cdot (1 - Pr_{succ}), \quad (14)$$

$$PDR = (1 - Pr[transmitter\ lying]) \cdot Pr_{succ} \cdot (1 - Pr[receiver\ lying]). \quad (15)$$

$$Pr[transmitter\ lying] = 1 - \frac{\tilde{P}r_{HTE} - PDR + PDR * Pr_{src3\_D}}{Pr_{src3\_D}}. \quad (16)$$

Overall Model: In this model we consider all the evidences with respect to the physical parameters are true and there may be some misbehaviours in the sender and receiver transmitting packets.

Enumeration: Since there are many hops Transmission evidence may actually vary in addition to the false behaviours of the sender and the receiver,so it may be differ from the actual work.If we use the single packet then the results are obtained quickly.But if we use heterogeneous analysis then so many parameters have to be considered.Heterogeneous analysis is quick and may provide accurate results where as the homogeneous approach provides inaccurateresults.

6. Calculations

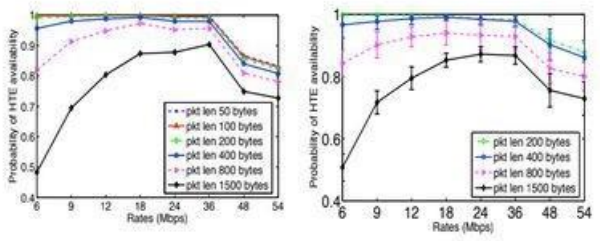
We consider both simulation and the experimental setup.We also examine the Transmission evidence availability on various scenarios.We also consider the false denial of the sender and the receiver using simulation.

N	10
P_t	3.16E-2 $watts$
P_n	3.16E-10 $watts$
λ	20 pkt/sec
R	100 m
η	1.0
α	2.0
Data packet length	50/100/200/400/800/1500 bytes
ACK length	20 bytes
Rates and SINR thresholds	See Table IV for the SINR thresholds and rates.

TABLE III: Default parameter settings

Rate	6	9	12	18	24	36	48	54
SINR	6.02	7.78	9.03	10.79	17.04	18.8	24.05	24.5

TABLE IV: 802.11a Rates (Mbps) and SINR thresholds (dB).



(a) Analytical (b) Simulation

Fig. 2: Hop-level TE availability probability

Experimental setup and simulation: We use the Network simulator .We observe that the nodes transmission takes place in the chaos manner,here we consider the average of all the nodes and we consider only selected

transmissions.The minimal portion of the calculated using all the transmission.

Bit rate and the length of the packet: For a bit-rate that remains constant ,we need very minimal packet length,minimal packet length leads to higher transmission evidence availability.If the bit rate varies the transmission evidence obtained is erroneous.If the packet length is maximum then the transmission evidence again becomes erroneous.
Volume of the traffic: We can vary the traffic.If the traffic is high then the transmission evidence decreases,if the traffic is low then the transmission evidence increases.
Limit for the retransmit: If the retransmission increases then the transmission evidence decreases.If the retransmission decreases then the transmission evidence increases.

PTE evidence: We consider for various traffic,bit length and hop counts the PTE availability.Generally if the packet length is minimum then the Path level TE availability is high,if the packet length is maximum then the Path level TE

availability decreases.If the hop count maximises then the PTE minimises.If the hop count minimises then the Packet length maximises.

HTE: The Hop level transmission evidence varies according to the bit rate,transmission rate and traffic rate,generally if any of these parameters are high then the then the transmission evidence decreases.

Assessment: By analysing both the experimental setup and the simulation we can get fairly good idea of the transmission evidence,we consider various parameters like network traffic,packet length,fading.This will definitely aid the probability of finding the malicious intent.

Ground Truth (%)	Assessment Results		
	avg dev (%)	min dev (%)	max dev (%)
transmitter 0	2.65	0.39	5.98
receiver 0	4.84	0.44	13.83
transmitter 10	2.05	0.00	1.05
receiver 0	4.20	0.00	11.77
transmitter 0	5.28	0.02	10.39
receiver 10	2.71	0.00	9.62
transmitter 10	1.80	0.18	6.08
receiver 10	1.84	0.38	5.88
transmitter 20	5.36	0.32	15.00
receiver 0	2.92	0.00	11.21
transmitter 0	1.36	0.00	8.49
receiver 20	2.32	0.35	9.24
transmitter 20	1.56	0.38	5.11
receiver 20	1.66	0.55	5.09
transmitter 40	3.87	0.29	10.89
receiver 0	2.59	0.00	9.09
transmitter 0	0.76	0.00	4.90
receiver 40	1.38	0.09	7.53
transmitter 40	0.99	0.26	3.11
receiver 40	1.01	0.16	3.05
transmitter 60	2.34	0.24	5.52
receiver 0	1.84	0.00	8.85
transmitter 0	0.23	0.00	1.42
receiver 60	1.89	0.50	5.20
transmitter 60	0.39	0.12	1.28
receiver 60	0.43	0.09	1.34

TABLE V: Assessments on transmitter and receiver lying

Analysis using TE: We consider the various possibilities of the receiver and the sender lying,both the simulation model and the experimental model are studied,they are again classified on their deviation in to higher estimate and lower estimate.Transmission evidence is calculated accordingly.

7. Conclusion:

In this model we use both the experimental setup and analytical setup.We use the analytical model in our forensic analysis.We then observe and analyse using elaborate calculations both theoretically and experimentally ,then based on it we determine if the packet discard behaviour by the sender and the receiver is due to he malicious intent ,here the probability is determined with high accuracy.

References

[1] J.Ning,Forensic Analysis of malicious and inducedpacket loss in wireless networks

[2] S.Marti,T.J.Giuli,K.Lai,andM.Baker,"Mitigatingroutingmisbehaviorinmobileadhocnetworks,"inProc.ACMMobiCom,2000,pp. 255–265.

[3] K.P.McGrathandJ.Nelson,"Monitoring&forensicanalysisforwireless networks," in Proc. Conf. Internet Surveillance Protection, 2006, pp.1–4.

[4] K. N. Ramach, E. M. Belding-royer, and K. C. Almeroth, "DAMON: Adistributedarchitectureformonitoringmultihopmobilenetworks," in Proc. IEEE SECON, 2004, pp.601–609.

[5] S.Yang,S.Vasudevan,andJ.Kurose,"Witness-baseddetectionofforwarding misbehaviors in wireless networks," UMass Computer Sci- ence Technical Report UM-CS-2009-001,2009.

[6] Rice University, Houston, TX, USA, "Wireless open-access research platform," [Online]. Available:http://warp.rice.edu/

[7] K.P.McGrathandJ.Nelson,"Flux:Aforensictimemachineforwireless networks," presented at the IEEE INFOCOM 2006 Poster and Demo Session2006.

[8] A.Adya,P.Bahl,R.Chandra,andL.Qiu,"Architectureandtechniques fordiagnosingfaultsinIEEE802.11infrastructurenetworks,"inProc. ACM MobiCom, 2004, pp.30–44.

[9] L.Qiu,P.Bahl,A.Rao,andL.Zhou,"Troubleshootingwirelessmesh networks," Comput. Commun. Rev., vol. 36, no. 5, pp. 17–28,2006.

[10] J.Yeo,M.Youssef,andA.Agrawala,"AframeworkforwirelessLAN monitoringanditsapplications,"inProc.ACMWorkshoponWireless Security: WiSe, 2004, pp.70–79.

[11] Y.-C. Cheng et al., "Jigsaw: Solving the puzzle of enterprise 802.11 analysis," in Proc. SIGCOMM, 2006, pp.39–50.

[12] R.Mahajan,M.Rodrig,D.Wetherall,andJ.Zahorjan,"Analyzing the MAC-level behavior of wireless networks in the wild," in Proc. SIG- COMM, 2006, pp.75–86.