Comparison of Data Transmission using Parameters in Normal and Covert Mode in VANETS

Amarpreet Singh
Associate Professor: Dept of CSE
ACET, Amritsar
IKG PTU, Jalandhar

Kimi Manchanda
M.Tech Scholar :Dept of CSE
PTURC-ACET,Amritsar
IKG PTU, Jalandhar

ABSTRACT

Accomplish the security gap in the VANETS network; one has to meet a new conception of transmitting the secure data with the covert channel communication. In this work the communication is going on with normal mode as well as secure mode. With the help of this covert communication the small amount of sensitive data entrenched into the legal packet and transmitting over the insecure network. One had to measured parameters like End to End Delay, Packet Drop, PDR (Packet delivery ratio) and Throughput on which basis the efficiency of these modes evaluated. In this paper, the comparison of the above parameters discussed in Normal mode as well as covert mode.

Keywords

End to End Delay, NS2, Packet Drop , Packet delivery Ratio and Throughput.

1. INTRODUCTION

IN VANETS networks, covert channels established for transmitting the sheltered data which are not easily detected by the invader or eavesdroppers. To protect the data from the attacker a scenario established in which data transmitted using two modes i.e. Normal Mode and Covert Mode. In this way, it is difficult to steal the data by the attacker. If the attacker will get success in breaking the security but in this case it is not sure that he will get sensitive data because one has to carry out a dual mode channel in this work based on bit selection mode and selection of bit is random in nature so the attacker is always in predicament to find the mode (i.e. the sender sends the data in normal or covert mode) of the data which is being transmitting over the secure channel. In this exertion the probability of receiving the sensitive data is very low down. Both the modes evaluated by using the parameters discussed above and comparison of data done in both the modes on the basis of output readings evaluated in the simulator named as NS2(Network Simulator). The comparison of the parameters discussed as below in the section 2.

2. COMPARISON OF PARAMETERS IN NORMAL MODE AS WELL AS COVERT MODE

2.1 Evaluation of End to End Delay

End to End delay means to calculate the total time taken by the sender node to the destination node for transmission of data. The formula used in the evaluation of END to END Delay is as follows:

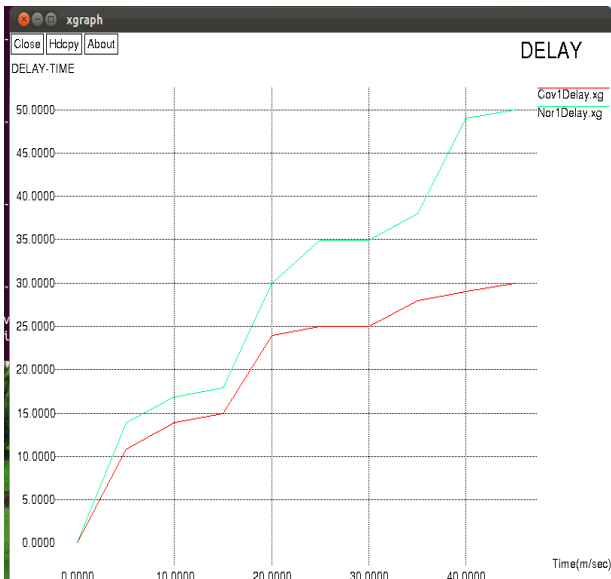The comparison of parameter End to End Delay in Normal Mode as well as covert mode is as shown below in Table 1.

Table 1 Output readings used for Comparison of the Parameter Delay in Covert Mode and the Normal Mode

Time(m/sec)	Time taken in Normal Mode	Time taken in Covert Mode	Delay reduced in Covert Mode
0	0	0	0
5	13.87	10.87	(13.87-10.87)=3ms
10	16.89	13.89	(16.89-13.89)=3ms
15	17.92	14.92	(17.92-14.92)=3ms
20	29.94	23.94	(29.94-23.94)=6ms
25	34.95	24.95	(34.95-24.95)=10ms
30	34.95	24.95	(34.95-24.95)=10ms
35	37.97	27.97	(37.97-27.97)=10ms
40	48.97	28.97	(48.97-28.97)=20ms
45	49.99	29.99	(49.99-29.99)=20ms

From these output readings, it can concluded that the delay reduced in covert mode (i.e. secure mode of transmission) as compared to the Normal mode as shown in the above table.

Evaluation of this objective done with the help of X-Graph in which time taken in the X-axis and Delay taken in the Y-axis of the covert as well as normal mode. The X-Graph which shows the End to end delay in normal communication and Covert communication is as shown below in Graph 1.

Delay of data = Time taken to send the data + Time taken to process the data + Time taken for the delivery of data

Graph 1: Delay Comparison between the Normal and Covert Mode

2.2 Packet Drop

Packet drop is that parameter which is used to calculate the number of packets lost in the transmission between the two nodes. Packet drop calculated with the help of formula written below:

Packet Drop = Packet Transmitted – Packet Delivered

The comparison of parameter Packet Drop in Normal Mode as well as covert mode is as shown below in Table 2.

Table 2 Output Readings used for Comparison of the Parameter Packet Drop in Covert Mode and the Normal Mode

Time(m/Sec)	Packet Drop in Normal Mode	Packet Drop in Covert Mode	Packet Drop reduced in Covert Mode
0	0	0	0
5	13.87	7.87	(13.87-7.87)=6
10	14.89	8.89	(14.89-8.89)=6
15	15.92	9.92	(15.92-9.92)=6
20	18.94	13.94	(18.94-13.94)=5
25	21.95	17.95	(21.95-17.95)=4
30	29.95	23.95	(29.95-23.95)=6
35	33.97	23.97	(33.97-23.97)=10
40	35.97	28.97	(35.97-28.97)=7
45	38.99	28.99	(38.99-28.99)=10

From these output readings, it can concluded that the Packet Drop reduced in covert mode (i.e. secure mode of transmission) as compared to the Normal mode as shown in the above table.

Evaluation of this objective done with the help of X-Graph in which time taken in the X-axis and Packet Drop readings taken in the Y-axis of the covert as well as normal mode. The X-Graph which shows the Packet Drop in normal communication and Covert communication is as shown below in Graph 2.

2.3 Packet Delivery Ratio

Packet delivery ratio is the ratio of summation of the number of packets received to summation of number of packets sent. The formula to calculate the packet delivery ratio is as mentioned below:

The comparison of parameter Packet Delivery Ratio in Normal Mode as well as covert mode is as shown below:

Packet Delivery Ratio = ∑ Number of packets received/∑ Number of packets sent * 100
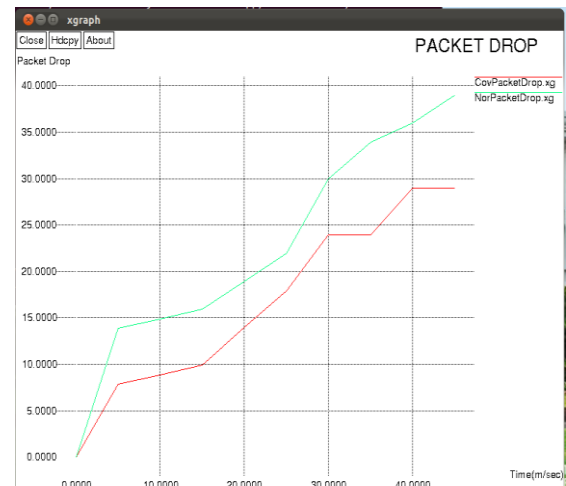
Graph 2: Packet Drop comparison between Normal and Covert Mode

The comparison of parameter Packet Delivery Ratio in Normal Mode as well as covert mode is as shown below in Table 3.
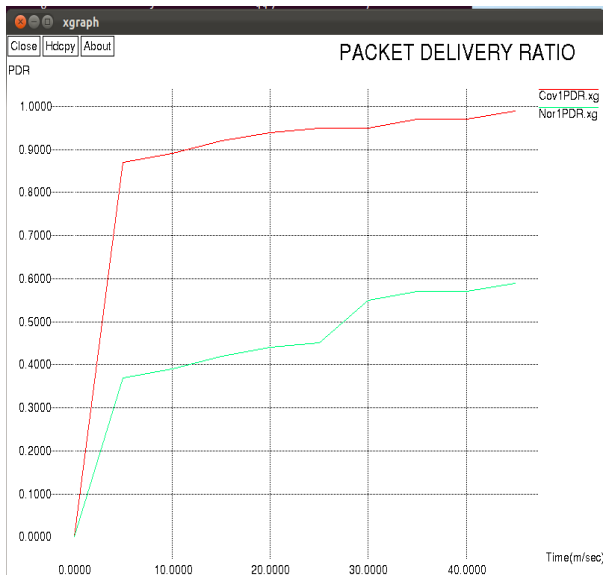
Table 3 Output readings used for comparison of the parameter Packet Delivery ratio in Covert mode and the normal mode

Time(m/sec)	PDR in Normal Mode	PDR in Covert Mode	PDR increased in Covert Mode
0	0	0	0
5	0.37	0.87	(0.87-0.37)=0.5
10	0.39	0.89	(0.89-0.39)=0.5
15	0.42	0.92	(0.92-0.42)=0.5
20	0.44	0.94	(0.94-0.44)=0.5
25	0.45	0.95	(0.95-0.45)=0.5
30	0.55	0.95	(0.95-0.55)=0.4
35	0.57	0.97	(0.97-0.57)=0.4
40	0.57	0.97	(0.97-0.57)=0.4
45	0.59	0.99	(0.99-0.59)=0.4

From these output readings, it can concluded that the Packet Delivery Ratio increased in covert mode (i.e. secure mode of transmission) as compared to the Normal mode as shown in the above table.

The evaluation of this objective done with the help of X-Graph in which time taken in the X-axis and PDR readings taken in the Y-axis of the covert as well as normal mode. The X-Graph which shows the Packet Delivery Ratio in normal communication and Covert communication is as shown below in Graph 3.

Graph 3: Packet Delivery Ratio Comparison between Normal and Covert Mode

2.4 Throughput

Throughput means how much data transferred in the communication scenario. It means that how much data or packets transmitted from the sender node to the destination node. Throughput defined as the ratio of summation of traffic received minus the traffic sent to the total data packets received. The formula for calculating the throughput is as follows:

The comparison of parameter Throughput in Normal Mode as well as covert mode is as shown below in Table 4.

Table 4 Output readings used for comparison of the parameter Packet drop in Covert mode and the normal mode

Time (m/sec)	Throughput in Normal Mode	Throughput in Covert Mode	Throughput increased in Covert Mode
0	0	0	0
5	27.87	87.87	(87.87-27.87)=60ms
10	48.89	88.89	(88.89-48.89)=40ms
15	48.92	98.92	(98.92-48.92)=50ms
20	53.94	103.94	(103.94-53.94)=50ms
25	63.95	123.95	(123.95-63.95)=60ms
30	64.95	124.95	(124.95-64.95)=60ms
35	67.97	127.97	(127.97-67.97)=60ms
40	68.97	128.97	(128.97-68.97)=60 ms
45	69.99	129.99	(129.99-69.99)=60 ms

From these output readings, it can concluded that the Throughput increased in covert mode (i.e. secure mode of transmission) as compared to the Normal mode as shown in the above table.

Evaluation of this objective done with the help of X-Graph in which time taken in the X-axis and Throughput readings taken in the Y-axis of the covert as well as normal mode. The X-Graph which shows the Throughput in normal communication and Covert communication is as shown below in Graph 4.

Throughput = $\sum$ (Traffic received – Traffic sent)/Total data packets received
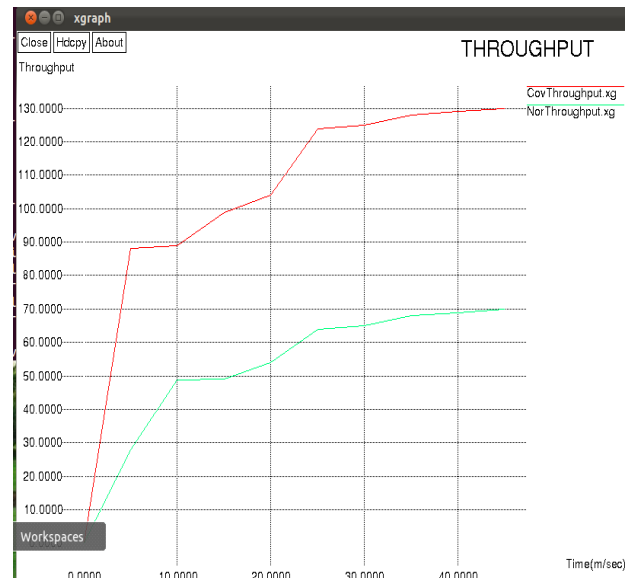
Graph 4: Throughput Comparison between Normal and Covert Mode

3. CONCLUSION

This paper is completed with the comparison of parameters between the two modes i.e. normal mode and covert mode It can concluded from the readings that the first parameter like End to end Delay reduced in the covert mode as compared to the Normal mode .The second parameter Packet drop which evaluated in both modes and from the evaluation results the packet drop is also reduced in the covert mode as compared to the Normal mode. From the readings of Packet Delivery ratio, it can concluded that the PDR is improved in Covert mode as compare to Normal mode after that from the comparison of last parameter throughput is that it is better in Covert mode.

4. FUTURE SCOPE

This work is advance extended with assistance of wired networks which means that Covert Channels implemented in the VANETS scenario by means of Wired networks because in that case the covert channels easily detected by the attacker. The detection by the attacker in wired mode is due to because these channels are immobile. If the attacker observes any

alteration in that scenario using this approach then the attacker can be effortlessly detected the covert data which is transmitting over the network. So, this analysis done further for transmission of private data on the network in wired mode and side by side the covert data can also be entrenched in the control messages like Route Request Header, Route Reply Header and error messages of the AODV protocol so that there is no need to entrench the data in the IPv6 Header. This work concluded for supplementary examination.

5. REFERENCES

[1] Fuentes J.M., BlascoJ., González A.I. and González L.,'' Applying Information Hiding in VANETs to Covertly Report Misbehaving Vehicles'', International Journal of Distributed Sensor Networks Volume 2014 (2014), Article ID 120626, 15 pages.

[2] Palomar E.,Fuentes J., Alcaide A.,'' Hindering false event dissemination with VANETS with proof-of-work mechanisms'', Department of Computer Science, Elsevier 2014.

[3] Tomandl A., Scheuer F. and Federrath H.,'' Simulation-based evaluation of techniques for privacy protection in VANETs'', 8th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), IEEE 2012.

[4] Abumansoor O. and Boukerche A.,''A Secure Cooperative Approach for Nonline-of-Sight Location Verification in VANET'', IEEE Transactions on Vehicular Technology, Vol. 61, no. 1, January 2012, IEEE 2012.

[5] Prashant K.M, Sharma V., Sahu G., Roberts A., Srivatava M. ,''An Overview of AODV Routing Protocol'', International Journal Of Engineering And Computer Science, IJES 2009

[6] M. Kimi and S.Amarpreet ,''Covert Communication in VANETS using Internet Protocol Header Bit'',International Journal of Computer Applications 123(17):10-14, August 2015.