Secure AODV using Symmetric Key Cryptography with Cyclic Chain Hash Function (CCHF)

Sitanshu Singh
School Of Information Technology, R.G.P.V
Bhopal (M.P) India

Sanjeev Sharma
School Of Information Technology, R.G.P.V
Bhopal (M.P) India

Santosh Sahu
School Of Information Technology, R.G.P.V
Bhopal (M.P) India

ABSTRACT
In this paper, we analyze the network performance with using Symmetric Key Cryptographic technique applying in AODV routing protocol with cyclic chain hash function (CCHF). Throughput and end to end delay of KK cryptographic (KKC) algorithm applying in AODV is less. If Symmetric Key Cryptographic technique used in AODV routing protocol with cyclic chain hash function has given maximum throughput and minimum end to end delay. In this dissertation, Key authentication is used in cyclic chain hash function. The proposed work we have implemented of the network performance. Shows the network performance of the proposed work is analysis of results. Network Simulator 2.34 is used for Simulation of results.

Keywords
Mobile Ad hoc Network, NS 2.34 Simulator, AODV Routing Protocol, Symmetric Key Cryptography, Hash Function

1. INTRODUCTION
AODV is perhaps the most well-known routing protocol for a MANET [4]. It is a reactive protocol: nodes in the network exchange routing information only when a communication must take place and keep this information up-to-date only as long as the communication lasts. Secure AODV is a security extension of the AODV routing protocol, based on Symmetric Key Cryptographic Techniques with the using of cyclic chain hash function. Symmetric Key Cryptography is work faster than Public Key Cryptography. Public key cryptography referred as RSA [12]. The hashing algorithm [5] is called the hash function probably the term is derived from the idea that the resulting hash value can be thought of as a mixed up version of the represented value.

1.1 Objectives
The Secure AODV [3] routing protocol is a security based on-demand routing protocol. The primary objectives are:
1. To perform the secure AODV with the using of security based techniques.

2. The second objectives are given maximum throughput and minimum end to end delay with the using of Symmetric Key Cryptographic techniques.

3. The third objectives are given minimum jitter effects with Symmetric Key Cryptographic technique.

2. RELATED WORK
Previously KK cryptographic (KKC) technique [1], Substitution Crypto, DES [2] were used to analyze throughput and end to end delay of wireless sensor network nodes. We observed this paper in the analysis that using Symmetric Key Cryptographic Technique implemented by AODV Routing Protocol throughput and end to end delay enhanced.

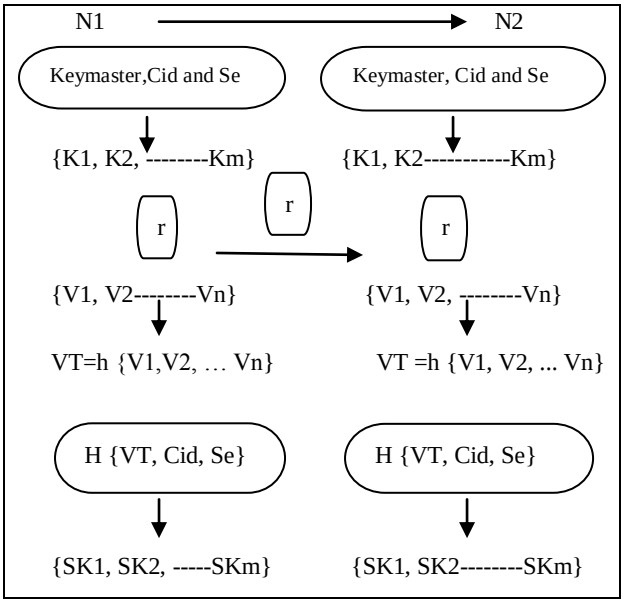
Cryptography is an emerging technology, which is important for the network security. Security and attack aspect of the cryptographic technique. Related work has concluded the issues of security [7], Network Performance tests and characteristics of the cipher texts. The simulation based network performance tests is to be done such as throughput, end to end delay, jitter effect and packet delivery ratio.

In the literature, there are many cryptographic algorithms in the mobile ad hoc network. By Jared cordasco and susanne wetzel [9] compare the security issues of the cryptographic and trust based method for routing security. A. santos, Edwards [10] have analyzed of the performance parameters, Throughput and end to end delay of the mobility for vehicular mechanism ad hoc network, and Wilson T.H. Woon [11] evaluate the performance of wireless 802.15.4 using simulation and test bed approach.

3. PROPOSED WORK AND IMPLEMENTATION
We have proposed a new methodology for generate of id key for the authentication of node. This method based on Cycle chain shift mechanism. In this mechanism the previous record of data are automatic destroy .That means the process of key generation maintain a process for independency of next value. Here we used some convention notation for our algorithm:-

(1) {N1,IN,N2} The set of notation represent the value of source node, intermediate node and destination node.
(2) Sk = Session key.
(3) (Ki)s = Secrete key.
(4) Se = Session in one Node to another Node.
(5) Cid = Communication and its identity
(6) VT = Represent value of communication, it equals h{V1,V2,V3}
(7) Token = a generated token
(8) (X) =message
(9) h(X) = hashed message

Key Generation Technique
Here discuss the dynamic key generate which is the main contribution in our proposed in addition to the type of confidential information shared between the two node. Our scheme require two set of keys to be generated at each party's side: secondary keys (Ki)s and session key (SK)s . (Ki)s are necessary to generate V values ,which are used as a security enhancement step to generate session keys. The node N1 will issue the intermediate node (IN) and a communication authentication once authenticated.



Block Diagram of Cycle Chain Shift Mechanism

The generation of (Ki)s is relies on the combination of three mentioned factors, Keymaster, Cid and Se as follows:-
Ki = h {Keymaster, Cid, Se}
Ki+1 = h {Cid, Se, Ki}
Ki+2 = h {Se, Ki, Ki+1}
Ki+3 = h {Ki, Ki+1, Ki+2}
Km = h {Km-3, Km-2, Km-1}

The first generation (Ki) relies on the existence of the three factors, whereas the next generation keys eliminate one of them after each generation step. The same shifting technique is applied for SKs generation as well. After the generation of (Ki) s, N1 and IN start generating V values (V1, V2, V3) as follows:

V1 = r mod (m-3)
V2 = r mod (m-2)
V3 = r mod (m-1)

Where m-3, m-2 and m-1 are hashed values of the last calculated secondary key (Ki). The generated V values will then be hashed to generate VT value, which is one of the pillars in generating (SK)s as follows:

VT = h {V1, V2, V3}

We will then use VT, Cid and Se to generate (SK)s as shown below :

SK1 = h {VT, Cid, Se}
SK2 = h {Cid, Se, SK1}
SK3 = h {Se, SK1, SK2}
SK4 = h {SK1, SK2, SK3}
SKm = h {SKm-3, SKm-2, SKm-1}

The main concept is to apply one hash algorithm with cyclic shifting of master secret each time a session key is generated.

3.1 Simulation Environment

How the simulations have been set up and finally it presents the results of the simulations. The simulations were conducted on an I3 processor and 2 GB RAM, running Linux open SUSE 11.0.Open SUSE 11.0 is version of RED HAT.

To be able to evaluate the implementation of the "Secure AODV using Symmetric Key Cryptography with Cyclic Chain Hash Function" in NS 2.34, some simulation scenarios must be run. all the simulation work is performed in NS 2 wireless network simulator version 2.34. Initially number of nodes are 21, Simulation time was taken 100000 milliseconds. All the scenarios have been designed in 2000m x 2000m area. Mobility model used is Random Way Point (RWP)[6]. In this model a mobile node is initially placed in a random location in the simulation area, and then moved in a randomly chosen direction between at a random speed between [$Speed_{Min}$, *SpeedMax*]. The movement proceeds for a specific amount of time or distance, and the process is repeated a predetermined number of times. We choose Min speed = 0 m/s, Max speed = 25m/s, and pause time = 5000 milliseconds. "Pause time is a time in which all nodes in network are motionless but transmission in continued".

All the simulation work was carried out using AODV routing protocol .Network traffic is provided by using Constant Bit Rate (CBR) sources. A CBR [8] traffic source provides a constant stream of packets throughput the whole simulation, thus further streaming the routing task.

Wireless network which we have used following values for different parameter:

Parameter	**Value**	**Description**
Number of Nodes	21	Network Nodes
Terrain Range	2000*2000	X,Y dimension of motion in Meter
Bandwidth	2 M bps	Nodes Bandwidth
Simulation Time	100000 milliseconds	Simulation Duration
Node Placement	Random	Node Placement Policy
Mobility	Random Way Point	Change Direction Randomly
Mobility	0-25 m/s	Mobility of Nodes
Traffic Model	CBR	Constant Bit Rate
Pause Time	5000 milliseconds	Non Mobility time at the terrain boundary
Routing Protocol	AODV	Base Routing Protocol for MANET

Table 1: Simulation Parameters for MANET in NS 2.34

4. PERFORMANCE MATRICS

In the simulations in the following section, the effects of different gateway advertisement intervals are evaluated. In comparing the gateway discovery approaches, the evaluation has been done according to the following four metrics:

4.1 Throughput is the measure of the number of packets successfully transmitted to their final destination per unit time. It is the ratio between the numbers of sent packets vs. received packets.

4.2 Packet delivery ratio is defined as the number of received data packets divided by the number of generated data packets.

4.3 End-to-End delay is defined as the time a data packet is received by the destination minus the time the data packet is generated by the source.

4.4 Jitter Effect signifies the packets from the source will reach the destination with different delays. A packet's delay varies with its position in the queues of the routers along the path between source and destination and this position can vary unpredictably.

5. RESULTS AND ANALYSIS

We have analyzed the results of the proposed work with the comparison of previous work.

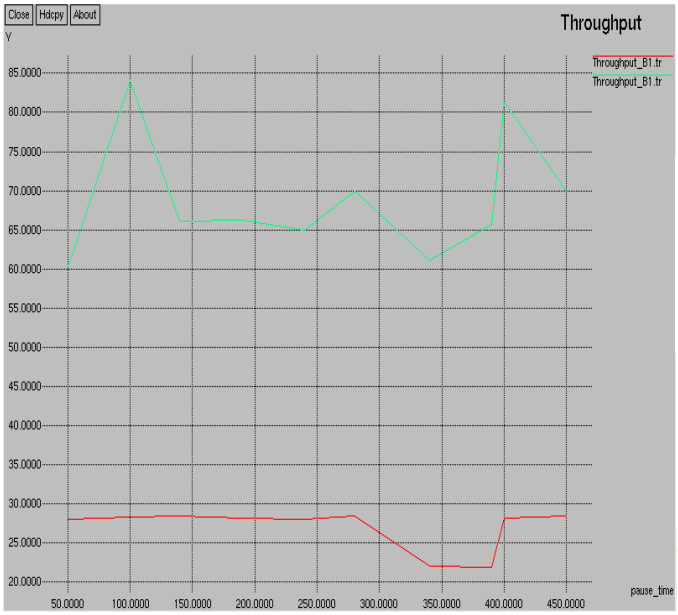


Fig. 1 Graph for Throughput

Figure 1 shows that the throughput of proposed model is maximum in comparison with KK cryptographic technique. Here, we have taken pause time as 5000 milliseconds and the no. of packets transmitted successfully is 6000 approximately. However, at the same pause time, the no. of packets transmitted successfully is 2750 approximately in case of KK cryptography. In same manner, when we have taken pause time as 10000 milliseconds, then packet transfer rate increases consistently in case of our proposed model, but in case of KK cryptographic technique the packet transfer rate is constant.

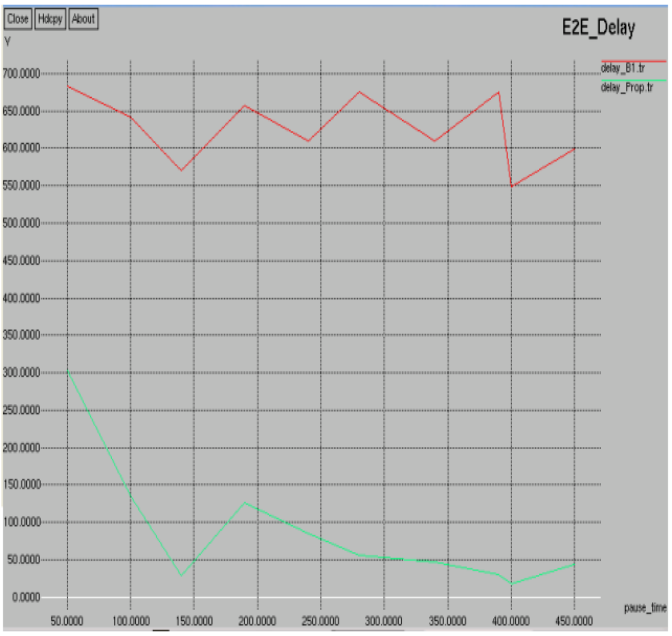


Fig. 2 Graph for End to End delay

Figure 2 shows that the end to end delay of proposed model is minimum with the comparison of KK cryptographic technique. Here we have taken pause time as 5000 milliseconds then the packet rate will be 30000 approximately in case of proposed model. However, at the same pause time packet rate will be 67500 approximately.

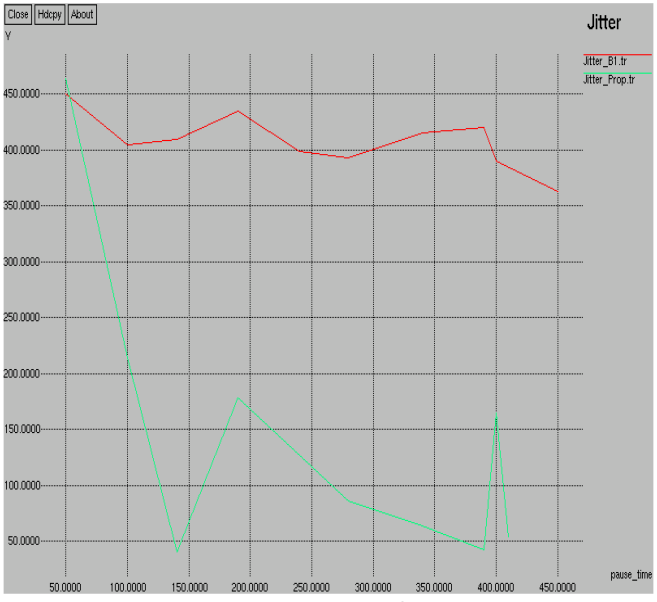


Fig. 3 Graph for Jitter

Figure 3 shows that the jitter affects are minimum in proposed work. We have taken pause time as 5000 milliseconds then the jitter effect are approximately same. But if we have taken pause time as 1500 milliseconds then the jitter effect is minimum of proposed work with the comparison of KK cryptographic technique.

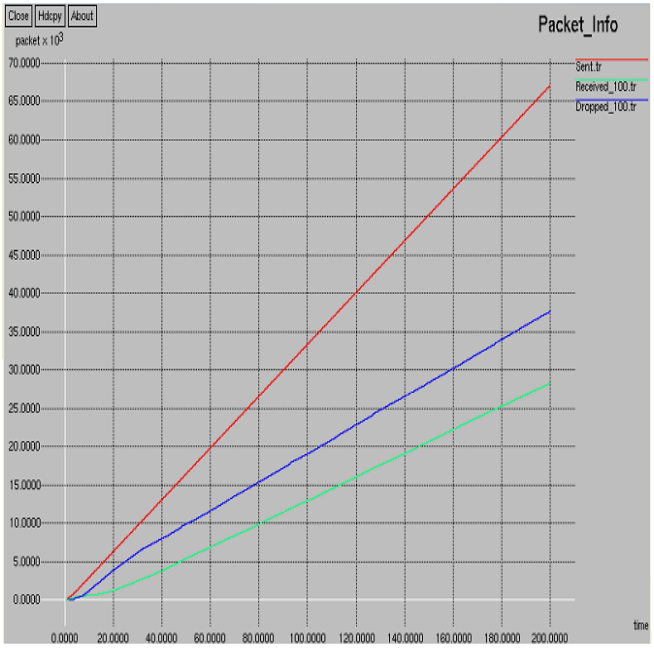


Fig. 4 Graph for Packet Information (KKC)

Figure 4 shows that the no. of packets send, no. of packets received and no. of packets dropped. When the time will be taken 20000 milliseconds then the no. of packets send by source to the destination is 670000 approximately. But the no. of packets received is 280000 approximately. That means the no. of packets dropped is 390000 approximately.

Number of packets received = Number of packets send – Number of packets dropped

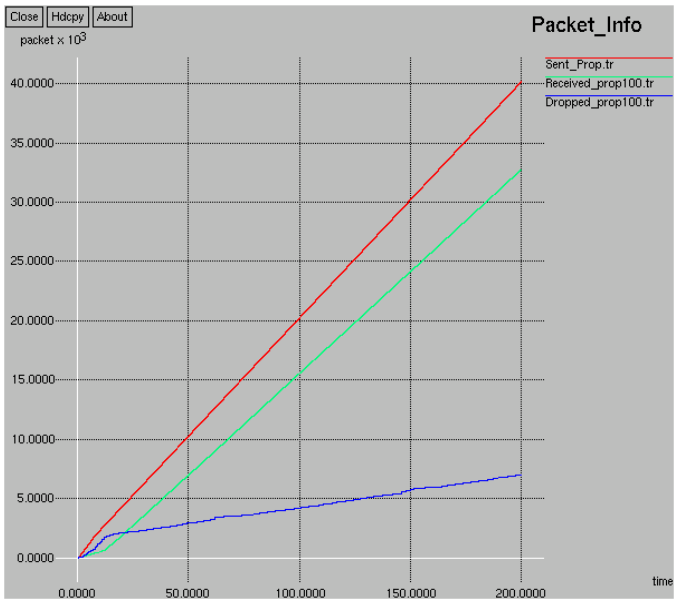


Fig. 5 Graph of Packet Information (CCHF)

Figure 5 shows that the no. of packets send, no. of packets received and no. of packets dropped. This figure shows no. of packets dropped is minimum to the previous figure which shows the previous work. When the time will be taken 20000 milliseconds then the no. of packets send by source to the destination is 400000 approximately. But the no. of packets received is 330000 approximately. That means the no. of packets dropped is 70000 approximately. In the proposed figure shows the minimum no. of packets dropped.

Number of packets received = Number of packets send – Number of packets dropped.

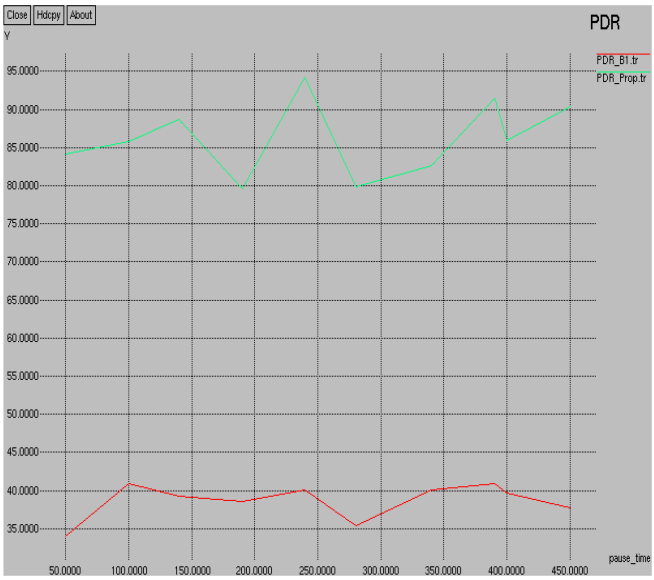


Fig. 6 Graph for Packet Delivery Ratio

Figure 6 shows that the packet delivery ratio (PDR) is maximum to the comparison of the previous Packet delivery ratio (PDR). If we have taken pause time are 5000 milliseconds then proposed Packet Delivery Ratio is maximum to the comparison of previous Packet Delivery Ratio (PDR).

PDR = Sum of the number of packet received / Sum of the number of packet send.

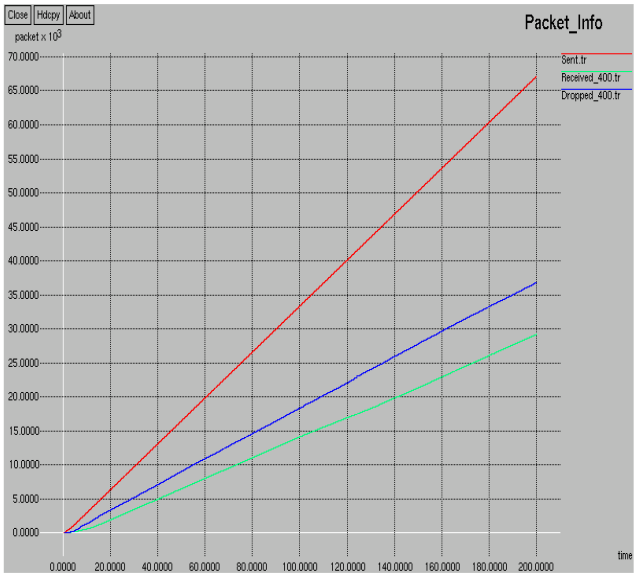


Fig. 7 Graph for Packet Information (KKC)

Figure 7 shows that again test of the packet information, the no. of packets send, no. of packets received and no. of packets dropped. When the time will be taken 20000 milliseconds then the no. of packets send by source to the destination is 670000 approximately. But the no. of packets received is 290000 approximately and the no. of packets dropped is

380000 approximately. That means give the same result approximately.

Number of packets received = Number of packets send – Number of packets dropped.

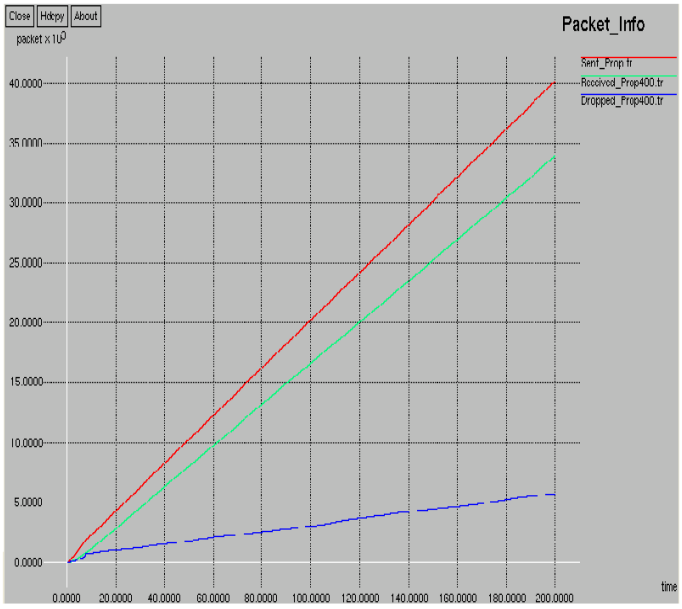


Fig. 8 Graph of Packet Information (CCHF)

Figure 8 shows that again test of the packet information, the no. of packets send, no. of packets received and no. of packets dropped. This figure shows no. of packets dropped is minimum to the previous figure which shows the previous work. When the time will be taken 20000 milliseconds then the no. of packets send by source to the destination is 400000 approximately. But the no. of packets received is 340000 approximately. That means the no. of packets dropped is 60000 approximately. In the proposed figure shows the minimum no. of packets dropped. That means give the same result approximately.

Number of packets received = Number of packets send – Number of packets dropped.

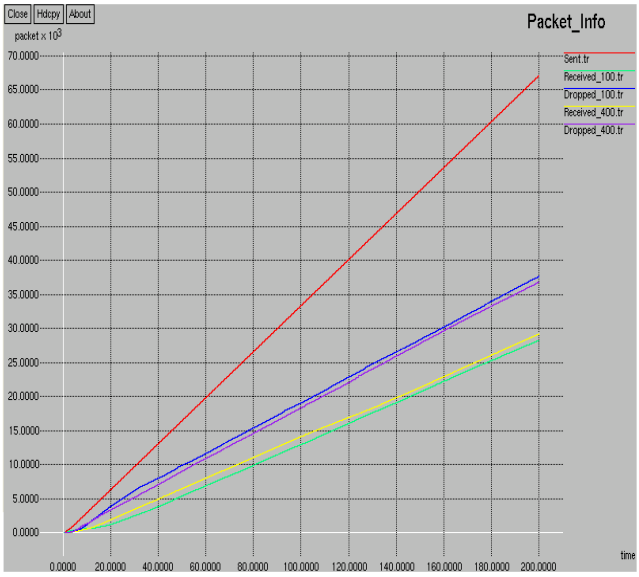


Fig. 9 Graph for Comparison of Packet Information (KKC)

Figure 9 shows that the comparisons of both results of previous work are approximately same.

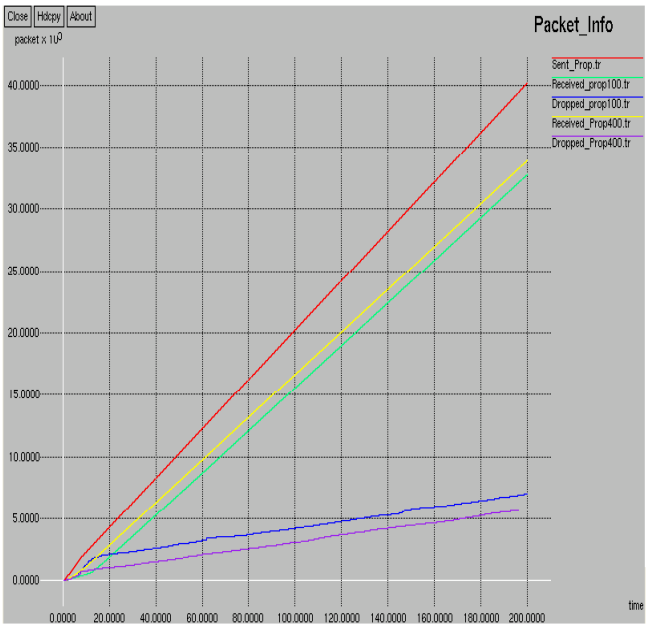


Fig. 10 Graph for Comparison of Packet Information (CCHF)

Figure 10 shows that the comparisons of both results of proposed work are approximately same. But the second result of proposed work shows the decrease of the no. of packets dropped.

6. CONCLUSION

In Cryptographic Techniques, our main motive is to find out maximum throughput and minimum end to end delay using Symmetric Key Cryptographic technique apply in AODV Routing Protocol in place of KK cryptographic technique, after my research work I found that the maximum throughput and end to end delay will be minimum.

In detail, previous work related to KK cryptographic technique use in AODV which give the results such as throughput and end to end delay are less with the comparison to proposed work Symmetric Key Cryptographic technique are applying in AODV protocol then the throughput will be maximum and end to end delay are minimum. So it is concluded that the proposed secure AODV Routing Protocol with using Symmetric Key Cryptographic Technique give the satisfied results.

7. FUTURE WORK

We can enhance the network performance with the using of different types of security based techniques. Which are used techniques to implement by AODV protocol with in network simulator. We can also use different environment for enhancement of Network Performance.

8. REFERANCES

[1] Yudhvir Singh, Dr. Yogesh Chaba "Security and Network Performance Evaluation of KK' Cryptographic Technique in Mobile Ad hoc Networks" IEEE International Advance Computing Conference (IACC 2009)

[2] Raymond G. Kammer, William M. Daley "U.S. DEPARTMENT OF COMMERCE/National Institute of

Standards and Technology" DATA ENCRYPTION STANDARD (DES), FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION, October 1999.

[3] Stephan Eichler, Christian Roman "Challenges of Secure Routing in MANETs: A Simulative Approach using" AODV-SEC Arcisstr. 21, 80333 München, Germany 2006.

[4] C. E. Perkins, E. M. Belding-Royer, and S. R. Das, "Ad hoc On-Demand Distance Vector (AODV) Routing," Internet Engineering Task Force (IETF) draft, November 2002. Available at http://www.ietf.org/internet-drafts/draft-ietf-manet-aodv-12.txt.

[5] S. Chang, M. Dworkin, Workshop Report, The First Cryptographic Hash Workshop, Report prepared, NIST 2005.

[6] E. Hyytiä, H. Koskinen, P. Lassila, A. Penttinen and J. Virtamo "Random Waypoint Model in Wireless Networks" University of Debrecen, Hungary, Networks and Algorithms: complexity in Physics and Computer Science Helsinki, June 16-19, 2005.

[7] Arun Kumar Bayya, Siddhartha Gupte, Yogesh Kumar Shukla ,Anil Garikapati "Security in Ad-hoc Networks" University of Kentucky, (December 2009).

[8] Naveen Choudhary "Constant Bit Rate Traffic Investigation for Network-on-Chip" International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-1, Issue-5, November 2011.

[9] Jared Cordasco and Susanne Wetzel "Cryptographic vs. Trust-based Methods for MANET Routing Security, STM 2007.

[10] A. Santos, A. Edwards, R.M. Edwards, N.L. Seed "Performance evalution of routing protocol in vehicular ad hoc network and ubiquitous computing" international journals of ad hoc network and ubiquitous computing, 2005, volume 1.

[11] Wilson T.H. Woon, Tat chee wan, "performance evaluation of IEEE 802.15.4 wireless multihop network simulation and tested approach", international journals of ad hoc network and ubiquitous computing, volume 3, issue-1, 2008.

[12]RSA-PSS {Provable secure RSA Signatures and their Implementation" Johannes Block http://rsapss.hboeck.de/ 2011