Secure Route Discovery Protocol with Enhanced Backtracking Technique for MANET

P. Panchanathan[1], E. R. Rakesh Kumar[2]
[1]Assistant Professor, Department of Computer Science, Annamalai University, Chidambaram, India
[2]Research Scholar, Department of Computer Science, Annamalai University, Chidambaram, India

***Abstract*: In Mobile Ad hoc Networks (MANET), malicious node detection and secure route discovery is one of the key issue for the establishment of secure communication among nodes. In this paper, we have proposed a secure route discovery protocol with enhanced backtracking technique for MANET. In our proposed scheme, an enhanced backtracking scheme is used to detect the malicious node based on the stability and path latencies of the node. To avoid lookup failure, timeout mechanism is used. Also, secure route is discovered by generating secure key and using Shamir's secret sharing technique.**

***Keywords*: Backtracking technique, Path latencies, Shamir's secret, Mobile Ad hoc Networks.**

1. Introduction

A. Mobile ad hoc network (MANET)

MANET is a multi-hop wireless network are composed of autonomous nodes that communicate with each other by forming dynamic topology such that nodes can easily join or leave the network at any time without any fixed infrastructure such as access points or base station and maintaining connections in a decentralized manner. The network over radio links are caused due to the self-organization of the mobile nodes. Each device in a MANET is free to move independently in any directions [1]. The infrastructure less property and the easy deployment along with the self-organizing nature makes them useful for many applications like military applications, mobile social networks, emergency deployment, intelligent transportation systems and fast response to disasters [2].

MANET also throws a security challenge due to their features of open medium, dynamically changing topologies, reliance on cooperative algorithms, absence of centralized monitoring points, and lack of clear lines of defense moderate bandwidth, limited battery power, computational power and limited resources. So mobile ad-hoc networks are vulnerable to several different attacks [3]

B. Collaborative Attacks in MANET

The collaborative attacks are defined as two or more types of attacks such as the black hole attacks and the wormhole attacks, which synchronized simultaneously in the network in a collaborative way [4]. It is a synchronized attacks where a system is distributed by more than one attacker simultaneously or involving two or more colluding nodes that can be processed using wired or wireless link and triggered by single or multiple attackers. Collaborative attacks (CA) occur when more than one attacker or running process synchronize their actions to disturb a target network but not necessarily in collaboration where every attack is launched by a specialized expertise. These attacks can be classified into two different categories [5].

Direct Collaborative Attacks: Here, the attacker nodes are already in existence in the original network or a malicious node joins the network or an internal node is compromised in the network. This kind of collaborative attacks can be referred to as direct collaborative attacks. For examples, Black hole and Wormhole attack.

Indirect Collaborative Attacks: The attacks in this category use different non-existent nodes in order to fake other nodes to redirect data packets to malicious node. This kind of collaborative attacks can be referred to as indirect collaborative attacks. For examples, Sybil and Routing table overflow attacks [6].

C. Collaborative attack detection in MANET

Collaborative attacks in ad hoc networks carriage challenges to the detection system. Malicious nodes may collude to conduct more complex and subtle attacks to prevent detection or identification. To detect against collaborative attacks essential that monitoring and detection agents collaborate efficiently. The collaboration should include each existing node in the network.

The main challenges include:

1) Integrating the information from multiple nodes in efficient manner.
2) For developing the attack detection mechanisms that should be robust against noise in the information.
3) For discovering the effective relationship between the range of network from which the information is integrated and the detection capabilities of the mechanisms.
4) Determining the trade-off between the detection granularity and the dynamics of the networks [7].

2. Literature Review

Reshma Lill Mathew and P. Petchimuthu [2] have proposed a collaborative watchdog based on contact dissemination with a log file system. The watchdog has detected a selfish node in the network then spread the information to other nodes when contact occurs. The detection of the contacts among the nodes is performed based on the node's watchdog for the detecting the selfish nodes. Log file system have used for reducing the detection time of the selfish node. After forwarding the packets from the neighbor node to next neighbour node, neighbor node could not overhear the packet dropping of next neighbour node either if transmission collides between source and neighbour node or neighbour node is not within the transmission range of next neighbour node. When this happens it could not provide the security.

Tao Gong and Bharat Bhargava [4] have proposed to defend the ad hoc network under collaborative attacks such as the black hole and the wormhole attacks using new tri-tier cooperative immunization from the inspiration of the human immune system. Tri-tier immunization includes native immune tier to recognize known attacks, adaptive immune tier to learn unknown attacks and parallel immune tier is built with the cloud-computing infrastructure for increasing both the efficiency and robustness of immune computation. The approach provides immunization to isolate the nodes under attacks by the network reconfiguration. Still it provides security reconfiguration is not possible.

Mahdi Nouri et. al [8] have proposed a collaborative technique for detecting a wormhole attack in that neighborhood using clustering. Monitor node initiates the detection process by passing messages between the nodes and depending on the messages received determine suspected nodes that sent to the monitor node. The suspected nodes receive at least a minimum number of votes or only one vote are finally detected as malicious nodes by inspecting the votes at monitor node and isolate malicious nodes from a group of nodes in routing process. But, using this technique not possible for detecting wormhole attack in the form of out of band attack. When there is congestion or collision, a node may be dropping packets due to overloaded, and so the algorithm will not work properly. And also if a monitor node continuously monitoring the detection process, it may cause exhausting of battery power because of overhead of being the monitor node.

Jian-Ming Chang et al [9] have proposed a cooperative bait detection scheme (CBDS) by designing a DSR based routing mechanism for detecting and preventing malicious nodes that attempts to launching gray hole/collaborative black hole attacks in MANETs that incorporates the advantages of both proactive and reactive response. Using a reverse tracing technique malicious nodes are detected and prevented from participating in the routing operation. When a significant drop occurs in the packet delivery ratio, an alarm is sent by the destination node back to the source node to trigger the detection mechanism again and the dynamic threshold value can be adjusted according to the network performance. However, if a lower the value is set, some of neighbors of the suspicious node may not be found.

Jaydip Sen et. al. [10] have proposed a distributed protocol for detection of packet dropping attack based on cooperative participation of the nodes in a MANET. The protocol works through cooperation of some security components that are present in each node in the networks such as monitor, trust collector, trust manager, trust propagator and whistle blower by using complementary relationship between cryptographic key distribution and intrusion detection activity. The redundancies in routing information make the detection scheme highly robust and secure and using of controlled flooding technique has very low communication overhead. However, after finding the malicious node it does not consider the technique for isolating the malicious node from participating in routing process.

Chang Wu Yu et. al [11] have proposed a distributed and cooperative mechanism for detecting potential multiple black hole nodes through collection of some local information. From the information, nodes evaluate that there exists any suspicious node among their one-hop neighbors. After finding the node as a suspicious, a cooperative procedure will be initiated to further check the potential black hole nodes. Then the global reaction is initiated to form a proper notification system to send warnings to the whole network. However, overhearing for collection of local information does not work always properly in situation like collision or weak signal. It leads to incorrect evaluation of the behaviour of the suspicious node.

Weichao Wang et. al [12] have developed a new mechanism for audit based detection of collaborative packet drop attacks using hash function based method to generate node behavioral proofs that contain information from both data traffic and forwarding paths. Intermediate node construct a Bloom filter based on the contents of the packets to generate the behavioral proof. It allows the system to successfully locate the routing segment in which packet drop attacks are conducted. However, other nodes cannot find the difference between an audit packet and a common data packet. Security is based on the value of its behavioral proof. So it is not efficient. If there is no malicious node all packets are delivered to destination without any packet dropping at intermediate node. So it does not analyze any scenario for delivery of packet ratio at destination.

Sukla Banerjee [13] have proposed detection and removal of cooperative black and gray hole attack in MANETs. The total data traffic is divided into small blocks for ensuring an end-to-end checking. Before sending any block source sends a prelude message to the destination to aware the incoming block. Flow of the traffic is monitored by the neighbors of each node. At the end of the transmission destination node sends postlude message containing the no of data packets received. Using this ack source node check whether the data loss is within the tolerable range, if not then the source node starts the process of detecting and removing malicious node by collecting the response from the monitoring nodes. However, the ability of this algorithm is based on finding the threshold probability of non-malicious packet drop. If the threshold probability for non-malicious packet drop is low, this algorithm identifies any malicious behaviour. But also it means that increases the false detection rate.

3. Problem Identification and Proposed Solution

In our previous paper, we have proposed a distributed trust based co-operative bait detection scheme for detecting collaborative attacks in MANET. Here using the trust value which is estimated using Bayesian interference, the Bait detection process is invoked. For this, the source node selects an adjacent node using the random scheduling process. This is the address of this adjacent node is used as bait destination address to bait malicious nodes in order to send a reply RREP message. By this the bait detection is raised. After the detection of malicious node the PDR value is ensured with the Threshold value, from this the again the bait detection process is triggered. Using the reverse tracing setup the malicious nodes are detected. From the random schedule table, the nodes with less trust value which is considered to be as un-trusted nodes are removed instantly.

A. *Overview*

Now as an extension work, instead of the reverse tracing technique, the enhanced backtracking chord protocol [15] can be applied. Once the malicious nodes are detected and confirmed, secure routes are discovered using the safety key generation and Shamir's secret sharing techniques [16].

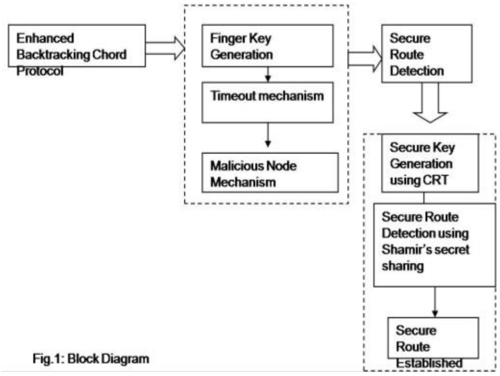

Fig. 1. Block diagram

Fig. 1 represents the proposed block diagram. In our proposed scheme, an enhanced backtracking scheme is used to detect the malicious node. For this first, Finger key is generated and updated in the Finger table based on the stability and path latencies. After that, timeout is set for each lookup request transmitted by the source. Based on the response received during defined timeout, malicious node is detected. After that, secure route is detected by secure key generation using CRT and Shamir's secret sharing technique.

B. *Enhanced Backtracking Chord Secured Protocol*

This section describes about the enhanced backtracking chord secured protocol to detect the malicious node without any delay and link breakage.

1) *Backtracking Chord*

In order to overcome the search failure caused by the link breakage due to sudden disappearance of the successor node, the Backtracking describes a timeout mechanism. In case a node have a source to request or to look for, it transmits a lookup request like in chord but also it sets a timeout to each and every query search. Moreover, if no reply packet is received within this timeout, the query is transmitted to the followed successor node in the table in spite of breaking the search process. The retransmission number is defined by the value of r, where r is a value between 0 and log R where R is the network size. This technique enhances the hit ratio.

2) *Enhanced Mobility Chord Protocol [15]*

It defines a novel lookup method for P2P applications in MANET. It develops a new path selection technique based on the combination of parameter such as nodes' mobility and application type in use, for which a standard threshold delay is defined. This unique protocol uses a periodic Ping dissemination scheme to attain information about the path latencies as a result of which the nodes' finger table will be updated periodically. This scheme makes the chord well adapted to dynamics network. This ping periodicity is carefully studied and observed in order to optimize the overhead, accuracy and freshness of the finger tables' entries. Based on the information provided by the ping messages, the path latencies are compared to the threshold delay defined by the application type. Only paths proposing latency inferior or equal to the defined threshold is taken into consideration. These accepted paths are sorted based on cost function. According to this protocol, for each key, the best path in terms of stability and latency is stored in the modified finger table and at most two other ones are stored.

3) *Initial Bait Setup Process*

Here the source node selects an adjacent node j_r within its one-hop neighborhood nodes and cooperate with this node by considering it address as the destination address of the bait $RREQ'$. The bait phase is triggered whenever the bait $RREQ'$ is sent prior looking for the initial routing path as shown in Fig. 3. The bait analysis process is described in the following steps:

a) If j_r node had not introduced a Blackhole attack, then once the source node has sent out the $RREQ'$, the other node has sent the RREP signifies that the malicious node is present in the reply routing. In Fig. 3 j_k and j_i are the malicious nodes as the RREP is transmitted by j_k and j_i. Hence, in order to detect the malicious node present in the route an enhanced backtracking chord protocol is initiated.

b) In case j_r has sent the RREP for the $RREQ'$ from the source node, there doesn't exist any other malicious node in the network except j_r.

c) If both j_r and other nodes in the network have sent RREP, then it shows that the malicious node is present in the route reply.

d) If the j_r does not send RREP purposely, then j_r is directly directed into Blackhole list by source node.

Once, the malicious node is suspected enhanced backtracking protocol is used to detect the malicious node which is described in the following section.

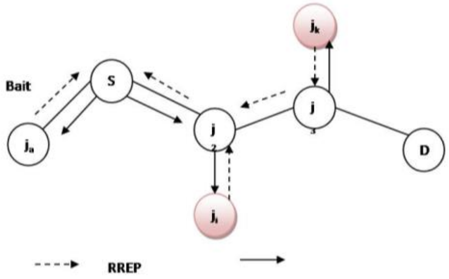

Fig. 2. Representation of Bait setup process

4) *Enhanced Backtracking Chord Protocol*

An enhanced backtracking chord protocol [1] is combination of backtracking and EMC. In order to decrease the failure ratio, the enhanced protocol includes the retransmission process provided by Backtracking and the path selection mechanism based on the stability node defined by EMC. Also, it includes the path selection based on the application required QoS to provide a successful search process for real time application such as VoIP.

In this enhanced protocol, the network's nodes periodically attain information about the path latencies and nodes' stability by sending ping messages. This information is stored in the finger table that not only include the Finger key and the successor node field but also two extra field containing stability values and the path delay as shown in Table 1.

Table 1
Finger Table

Finger Key	Successor Node Field	Node Stability	Path Delay

Based on the path diversity incorporated on EMC, each key can be reached by maximum three paths. After that, according to modified finger table, the sender node transmits a lookup request to the successor node providing the best path stability and latency based on the cost function defined by EMC.

Similar to Backtracking Chord, a timeout is set once the lookup request is transmitted. In case, no reply is received during this timeout period, the source node re-transmits the request to another successor node. After that, it verifies its modified Finger table for the successor node entry. First, it verifies whether there is another defined node giving the second best path performance to the resource or key looked for. In case this node is found, then the lookup request is sent to this node. Else, the query is sent to the next stage successor based on Backtracking Chord scheme. The node with greater stability without any delay is considered and updated in the modified table. In this way, the malicious nodes are detected and only the trusted nodes are updated in the Finger Table entry. The Fig.3 represents the flowchart of Enhanced Backtracking Chord. R represents the retransmission number.

Algorithm for Enhanced Backtracking Chord Protocol:

```
Node searching for the key S
Transmit a lookup request
Timeout is set
If reply is received during timeout
Then lookup is success
Else if
Source node search for the alternate successor node for the key S.
If alternate successor node reply during timeout
Then lookup success
Else lookup fail
Source re-transmits to the next successor node in the finger table
If successor node in the network in the finger table reply during timeout
Then lookup success
Else lookup fail
If last successor node in the Finger table
Then lookup fail
Else lookup success.
```

C. *Secure Route Discovery*

After the detection of malicious node using enhanced backtracking record, secure routes are discovered between the source node and destination node. This section describes about the secure route discovery based on safety key generation using CRT and Secure Route Detection scheme using Shamir's secret sharing. Chinese remainder theorem (CRT) uses the result about congruence in number theory and its simplification in abstract algebra.

1) *Secure Key Generation using CRT [16]*

Secure Key (SK) is a key which is used to detect secure routes among all available routes found based on the Finger table entry. Source node generates n integers $k_1, k_2, \ldots\ldots\ldots\ldots\ldots\ldots k_n$ such that $\gcd(k_i, k_j) = 1$. Then this key is generated using following equations:

$$l_i = k / k_i, m_i \equiv z_i^{-1} (\mathrm{mod}\, k_i)\, and\, l \equiv a_1 (\mathrm{mod}\, k_1) \equiv a_2 (\mathrm{mod}\, k_2) \ldots\ldots\ldots\ldots \equiv a_n \,\mathrm{mod}(k_n)$$

Here $(\mathrm{mod}\, k_i)$ stands for moduler multiplicative inverse operation

$$SK = a_1 m_1 l_1 + \ldots\ldots\ldots\ldots\ldots + a_n m_n l_n \tag{1}$$

Before transmitting message source node S generates SK_S using CRT.

2) *Secure Route Detection Technique using Shamir's secret sharing [16]*

According to the proposed scheme, the source node S divides the Secure Key SK_S into n parts, where n represents number of available routes from source to destination. After that, source node generates a polynomial

$P(x) of$ degree $floor(n/2)-1=b-1$ such that,

$$P(x)=a_0+a_1(x)+a_2x^2+.......a_{b-1}x^{b-1} \tag{2}$$

Where $a_0, a_1, ...a_{b-1}$ are set of integers

Source node generates n number of points from this polynomial which are $(x_0,y_0);(x_1,y_1);.................(x_{n-1},y_{n-1})$ and transmits each of these points in encrypted form [section 3.3.3] through each among n different available route to destination node.

After that the destination node decrypts [section 3.3.4] and again encrypts those points and sends to the source by backtracking in the same route from which it received the message.

Now source node decrypts those n points and takes any b points among them to regenerate the polynomial $P_1(x)$ using Lagrange's Interpolation such that

$$P_1(x)=\sum_{s=0}^{b-1} y_s \Pi_{i=0,i\neq s}^{b-1} \frac{x-x_i}{x_s-x_i} \tag{3}$$

The first constant part of $P_1(x)$ is called SK_1. If, $SK_S = SK_1$, those b points are valid points and the routes used by the b points are also valid and hence it is secured. In Fig. 3, point 2, 9, 8 are the valid points. Else, at least one of the routes used by those b points is not secured. ${}^nC_b$ number of combination are available for calculating secure key. Those combinations generating exact value of secure key will correspond to the respective secure routes.

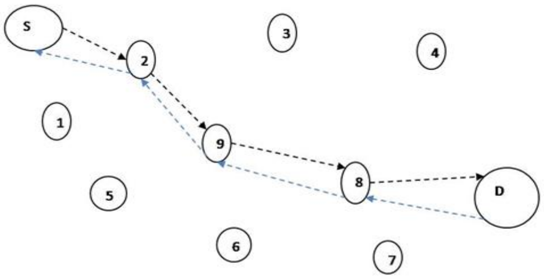

Fig. 3. Secure route detection scheme

3) Encryption Technique using RSA at source node

When source node wants to encrypt message E to Cipher text T for transmitting to the destination node, it uses public key of destination node using RSA in the way described as below:

$$T = E^v(\mathrm{mod}U) \tag{4}$$

4) Decryption using CRT at destination node

Once the destination node receives the encrypted message, then it decrypts the encrypted message using CRT in the following way:

$$cg = c\,\mathrm{mod}(g-1)$$
$$ch = c\,\mathrm{mod}(h-1)$$
$$h_{inv} = h^{-1}\,\mathrm{mod}\,g$$
$$k_1 = t^{cg}\,\mathrm{mod}\,g$$
$$k_2 = t^{ch}\,\mathrm{mod}\,h$$
$$q = (h_{inv}(k_1-k_2))\,\mathrm{mod}\,g$$
$$E = k_2 + q*h$$

D. The Overall Algorithm

// Enhanced Backtracking Chord//
1. Network nodes send ping messages
2. Attain the information from finger table
3. Modify the finger table
4. Source node transmits lookup request to the successor node
5. Timeout is set
6. If no reply is received
7. Then source node re-transmits the request to another successor node
8. It verifies modified Finger table for this entry
9. It verifies the node is second best path performance to the key looked for
10. Else
11. Query is sent to the next stage successor node
// Secure Route Discovery//
12. Secure key generation
13. Source node divides Secure Key into n parts
14. Source node generates n number of point using defined polynomial
15. Source node transmits each points in encrypted form
16. Destination node decrypts the message and again encrypts those points and send those point to the source by backtracking in the same path
17. Source node decrypts those points
18. If
19. Then the points are valid and secured
20. Else at least one point is not secured
21. Estimate secure key using combination
22. These combination gives exact secure key to the respective secure route

4. Simulation results

A. Simulation model and parameters

The Network Simulator (NS-2) [18], is used to simulate the proposed architecture. In the simulation, 200 mobile nodes move in a 1000-meter x 1000-meter region for 50 seconds of simulation time. All nodes have the same transmission range of 250 meters. The simulated traffic is Constant Bit Rate (CBR).

The simulation settings and parameters are summarized in table.

Table 2
Simulation settings and parameters

No. of Nodes	200
Area Size	1000 X 1000
Mac	IEEE 802.11
Transmission Range	250m
Simulation Time	50 sec
Traffic Source	CBR
Packet Size	512
Rate	150kb
Attackers	5,10,15,20 and 25

B. *Performance Metrics*

The proposed Secure Route Discovery Protocol with Enhanced Backtracking Technique (SRDPEB) is compared with the CBDS technique [11]. The performance is evaluated mainly, according to the following metrics.

- Packet Delivery Ratio: It is the ratio between the number of packets received and the number of packets sent.
- Packet Drop: It refers the average number of packets dropped during the transmission
- Overhead: It is the number of router packets received by the receiver during the transmission.

C. *Results*

Scen-1:

1) *Based on Attackers*

In our first experiment we vary the number of attackers as 5, 10, 15, 20 and 25.

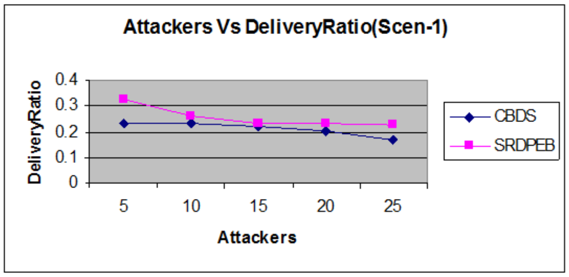

Fig. 4. Attackers vs. Delivery Ratio

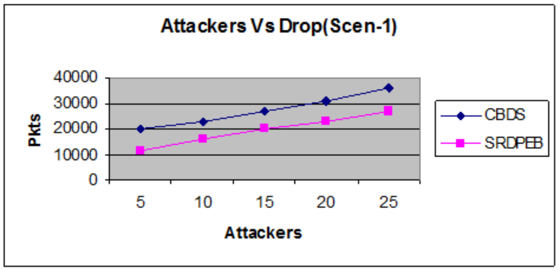

Fig. 5. Attackers vs. Drop

Figure 4 shows the delivery ratio of SRDPEB and CBDS techniques for different number of attacker scenario. We can conclude that the delivery ratio of our proposed SRDPEB approach has 17% of higher than CBDS approach.

Figure 5 shows the drop of SRDPEB and CBDS techniques for different number of attacker scenario. We can conclude that the drop of our proposed SRDPEB approach has 30% of less than CBDS approach.

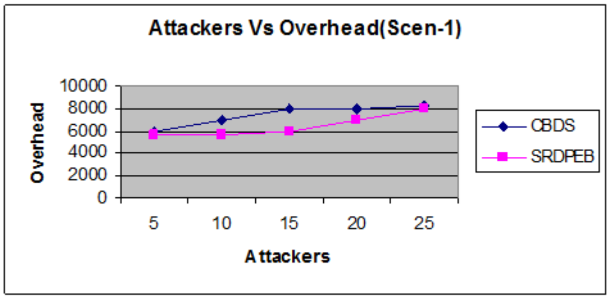

Fig. 6. Attackers vs. Overhead

Figure 6 shows the overhead of SRDPEB and CBDS techniques for different number of attacker scenario. We can conclude that the overhead of our proposed SRDPEB approach has 13% of less than CBDS approach.

Scen-2:

2) *Based on Attackers*

In our first experiment we vary the number of attackers as 5, 10, 15, 20 and 25.

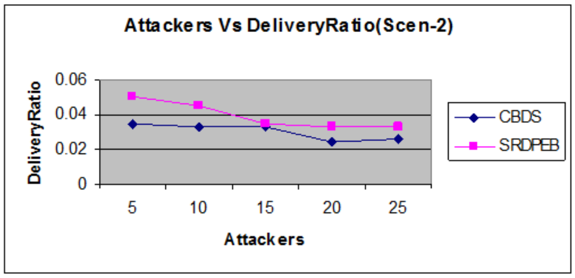

Fig. 7. Attackers vs. Delivery Ratio

Figure 7 shows the delivery ratio of SRDPEB and CBDS techniques for different number of attacker scenario. We can conclude that the delivery ratio of our proposed SRDPEB approach has 23% of higher than CBDS approach.

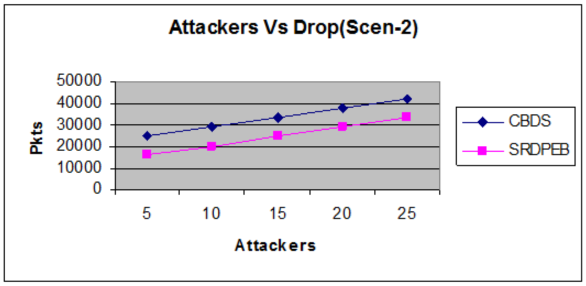

Fig. 8. Attackers vs. Drop

Figure 8 shows the drop of SRDPEB and CBDS techniques for different number of attacker scenario. We can conclude that the drop of our proposed SRDPEB approach has 27% of less than CBDS approach.

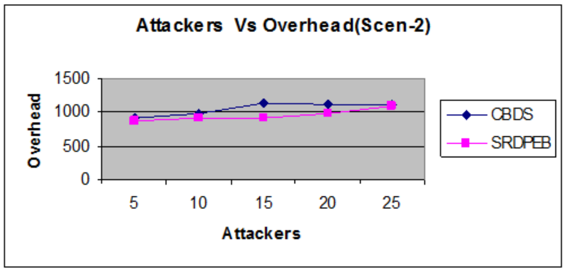

Fig. 9. Attackers vs. Overhead

Figure 9 shows the overhead of SRDPEB and CBDS techniques for different number of attacker scenario. We can conclude that the overhead of our proposed SRDPEB approach has 9% of less than CBDS approach.

5. Conclusion

In this paper, we have proposed a secure route discovery protocol with enhanced backtracking technique for MANET. Here, an enhanced backtracking chord protocol is used to detect the malicious node present in the network. Based on the stability and path latencies the node is updated in the table for the confirmation about the node. After that based on the, timeout mechanism the reliability of the node and path selected is found. After the detection of malicious node, secure route is discovered. To achieve this, a secure key is generated using CRT. A secure route is detected by implementing Shamir's secret sharing technique which helps to detect the valid points to establish a secure communication.

References

[1] Meenakshi Patel and Sanjay Sharma, "Detection of Malicious Attack in MANET A Behavioral Approach", IEEE 3rd International Advance Computing Conference (IACC), pp. 388-393, 2012.

[2] Reshma Lill Mathew, P. Petchimuthu, "Detecting Selfish Nodes in MANETs Using Collaborative Watchdogs", International Journal of Advanced Research in Computer Science and Software Engineering, vol. 3, Issue 3, March 2013.

[3] Umesh Kumar Singh, Kailash Phuleria, Shailja Sharma and D.N. Goswami, "An analysis of Security Attacks found in Mobile Ad-hoc Network", International Journal of Scientific & Engineering Research, vol. 5, Issue 5, May 2014.

[4] Tao Gong and Bharat Bhargava, "Immunizing mobile ad hoc networks against collaborative attacks using cooperative immune model", Security and Communication Networks, vol. 6, Issue 1, pp. 58–68, January 2013.

[5] Ajay Dureja and Vandna Dahiya, "Performance Evaluation of Collaborative Attacks in Manet", Journal of Computer Science and Information Technology, vol. 3, Issue. 7, pp. 457-465, July 2014.

[6] Cong Hoan Vu and Adeyinka Soneye, "An Analysis of Collaborative Attacks on Mobile Ad hoc networks", LAP LAMBERT Academic Publishing, June 2009.

[7] Bharat Bhargava, Ruy de Oliveira, Yu Zhang and Nwokedi C. Idika, "Addressing Collaborative Attacks and Defense in Ad Hoc Wireless Networks", 29th IEEE International Conference on Distributed Computing Systems Workshops, pp. 447-450, 2009.

[8] Mahdi Nouri, Somayeh Abazari Aghdam and Sajjad Abazari Aghdam, "Collaborative Techniques for Detecting Wormhole Attack in MANETs", International Conference onResearch and Innovation in Information Systems (ICRIIS), pp. 1-6, 2011.

[9] Jian-Ming Chang, Po-Chun Tsou, Isaac Woungang, Han-Chieh Chao, and Chin-Feng Lai, "Defending Against Collaborative Attacks by Malicious Nodes in MANETs: A Cooperative Bait Detection Approach", IEEE systems journal, vol. PP, Issue: 99, pp. 1-11, 2014.

[10] JaydipSen, M. Girish Chandra, P. Balamuralidhar, Harihara and S.G., Harish Reddy, "A Distributed Protocol for Detection of Packet Dropping Attack in Mobile Ad Hoc Networks", IEEE International Conference on Telecommunications and Malaysia International Conference on Communications, pp. 75-80, 2007.

[11] Chang Wu Yu, Tung-Kuang Wu, ReiHeng Cheng and Shun Chao Chang, "A Distributed and Cooperative Black Hole Node Detection and Elimination Mechanism for Ad Hoc Networks", Emerging Technologies in Knowledge Discovery and Data Mining Lecture Notes in Computer Science, vol. 4819, pp. 538-549, 2007.

[12] Weichao Wang, Bharat Bhargava and Mark Linderman, "Defending against Collaborative Packet Drop Attacks on MANETs", 2nd International Workshop on Dependable Network Computing and Mobile Systems (DNCMS), vol. 27, 2009.

[13] Sukla Banerjee, "Detection / Removal of Cooperative Black and Gray Hole Attack in Mobile Ad-Hoc Networks", In proceedings of the world congress on engineering and computer science (WCECS), pp. 22-24, 2008.

[14] Zhexiong Wei, Helen Tang, F. Richard Yu, Maoyu Wang, and Peter Mason, "Security Enhancements for Mobile Ad Hoc Networks with Trust Management Using Uncertain Reasoning", IEEE Transactions on Vehicular Technology, 2014.

[15] Mariem Thaalbi, Nabil Tabbane, Tarek Bejaoui, Ahmed Meddahi," Enhanced Backtracking Chord Protocol for Mobile Ad hoc Networks", IEEE Second International Conference on Communications and Information Technology, 2012.

[16] Ditipriya Sinha, Uma Bhattacharya, Rituparna Chaki, "RSRP: A Robust Secure Routing Protocol in MANET", Foundations of computing and decision sciences, vol. 39, 2014.

[17] https://www.eecis.udel.edu/~mills/time.html.

[18] Network Simulator: http:///www.isi.edu/nsnam/ns