World Academy of Science, Engineering and Technology
International Journal of Computer and Information Engineering
Vol:9, No:6, 2015

Secure Low-Bandwidth Video Streaming through Reliable Multipath Propagation in MANETs

S. Mohideen Badhusha, K. Duraiswamy

Open Science Index, Computer and Information Engineering Vol:9, No:6, 2015 publications.waset.org/10002105.pdf

***Abstract*—**Most of the existing video streaming protocols provide video services without considering security aspects in decentralized mobile ad-hoc networks. The security policies adapted to the currently existing non-streaming protocols, do not comply with the live video streaming protocols resulting in considerable vulnerability, high bandwidth consumption and unreliability which cause severe security threats, low bandwidth and error prone transmission respectively in video streaming applications. Therefore a synergized methodology is required to reduce vulnerability and bandwidth consumption, and enhance reliability in the video streaming applications in MANET. To ensure the security measures with reduced bandwidth consumption and improve reliability of the video streaming applications, a Secure Low-bandwidth Video Streaming through Reliable Multipath Propagation (SLVRMP) protocol architecture has been proposed by incorporating the two algorithms namely Secure Low-bandwidth Video Streaming Algorithm and Reliable Secure Multipath Propagation Algorithm using Layered Video Coding in non-overlapping zone routing network topology. The performances of the proposed system are compared to those of the other existing secure multipath protocols Sec-MR, SPREAD using NS 2.34 and the simulation results show that the performances of the proposed system get considerably improved.

***Keywords*—**Bandwidth consumption, layered video coding, multipath propagation, reliability, security threats, video streaming applications, vulnerability.

I. Introduction

A mobile ad hoc network is a group of wireless, self-configurable, dynamic nodes which are capable of organizing themselves in any topology to find route and relay packets from source to destination without a centralized administrator and infrastructure. The major issues of video streaming in MANETs are node mobility, dynamic change in topology, multipath shadowing and fading, interference and high bandwidth consumption. The dynamic change in topology causes periodic connectivity that results in large packet loss. Many issues of video streaming and the techniques to solve them have been discussed in [1]. Video streaming in real time requires special techniques that can overcome the losses of packets in unreliable networks [2]. The security policies adapted to non-streaming applications are not suitable for live streaming applications. Compared to fixed networks, MANET is more vulnerable to security attacks because of its exclusive characteristics, such as open medium, dynamic topology, resource constraints and lack of centralized management point [3]. Though applications of MANETs include mobile computing, search and rescue, and disaster recovery, the problem of securing MANETs is still in its infancy [4]. Inevitably, a variety of attacks have targeted the network layer, such as Wormhole and Byzantine attacks, and these have been identified and studied in the literature [5]. In these attacks, attackers inject themselves onto the path between the source and destination, thereby controlling the network traffic flow. For example, traffic packets may be forwarded through a non-optimal path, which can result in significant delay. Consequently, the attackers are able to introduce severe network congestion and performance degradation [6]. Though the existing proposals mainly address the security vigor of the design, they largely ignore the aspect of network performance [7]. The video streaming over mobile ad hoc networks is more challenging than that of other networks due to dynamic changes in the network topology with unreliable wireless channels [8], [9]. Though ZRP [10] establishes a network that works effectively by combining proactive and reactive approaches, the size of the zone is uncertain. If the size of the zone is too large, then there will be too many updates nearly as proactive method. On the other hand, if it is too small, it will resort to a reactive method. It will be difficult to have variable size zones and formation of dynamic zones makes it difficult to apply it in the live video streaming applications directly without any modification. The performance of the video streaming service gets considerably improved with the deployment of Border Relay Nodes (BRNs) in the boundary of non-overlapping zones to route the video packets towards the destination. To improve reliability and ensure security with low bandwidth consumption for providing a secure video streaming service through reliable multipath, the non-overlapping zone routing network topology as shown in Fig. 1 is used in this paper.

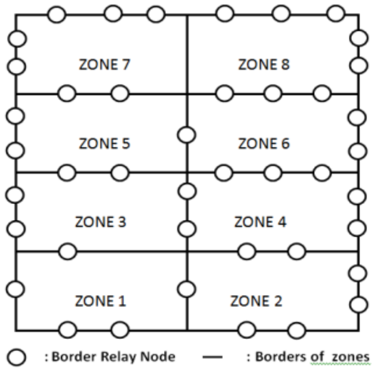

Fig. 1 Non-overlapping zone routing network topology

S. Mohideen Badhusha and Dr. K. Duraiswamy are with the Computer Science and Engineering Department, from K.S. Rangasamy College of Technology, India (e-mail: badhusha.sm@gmail.com, drkduraiswamy@yahoo.co.in).

Open Science Index, Computer and Information Engineering Vol:9, No:6, 2015 publications.waset.org/10002105.pdf

A. Objectives

In this paper, we have designed an amicable networking architecture using non-overlapping zone routing network topology. In this regard, it is important to consider the following three aspects as major objectives for developing a secure, low-bandwidth consuming and reliable video streaming application in MANET.

- To ensure the primary security aspects for mobile ad hoc networks in video streaming applications and find the ways and means to adopt them
- To overcome the problem of high bandwidth consumption of video streaming applications in MANET
- To adopt reliable video streaming without causing errors and loss of data through reliable multipath propagation

B. Accomplishments

To accomplish the first objective, i.e., ensuring the primary security aspects for MANETs in video streaming applications, the following three security aspects of the network are considered and adopted in the proposed work.

- Confidentiality
- Integrity
- Authentication

Confidentiality is the concept that ensures the privacy of the data exchanged that is the exchanged information should be revealed to only authorized persons and hidden to other members. It can be established through encryption of the data so that it cannot be intercepted and accessed by any unauthorized persons during transmission.

It can be established by encryption to ensure the privacy of the transmitted data. In the public key cryptography that is unlike symmetric-key cryptography, there are distinctive keys in asymmetric-key cryptography namely private key and public key. If encryption and decryption are thought of as locking and unlocking padlocks with keys, then the padlock that is locked with a public key can be unlocked only with the corresponding private key.

Integrity as a concept means that there should be a resistance to alteration or substitution of data, and/or such changes are detected and provable. The information should not be changed except by an authorized agent. This usually involves the use of checksums, one-way hashes and other algorithmic validation of the data. Whether the data might be changed by accident or malice, preventing that change is the primary concern, and detecting if it has changed or not is a secondary one.

To check the integrity of a message or document, we run the cryptographic hash function again and compare the new message digest with the previous one. If both are the same, we are sure that the original message has not been changed. A message digest guarantees the integrity of a message—it guarantees that the message has not been changed. A message digest, however, does not authenticate the sender of the message.

Authentication is the process of authenticity which assures that a message, transaction, or another exchange of information is from the source it claims to be from. Authenticity involves proof of identity of the sender of a message or data. The lack of authenticity leads to problems such as spam, e-mail phishing, website redirection, browser hijacking and other attacks such as man-in-the-middle attacks.

From the analysis, it is observed that it is highly expensive and ineffective to implement all these security aspects which are adaptable for infrastructure networks like cellular networks, directly in live video streaming applications of Mobile ad hoc Networking Environment. Therefore, they can be adopted indirectly by propagating the video packets through multipath with symmetric key encryption technique and generating a highly secure instant session key through public key double encryption technique. These two techniques ensure confidentiality and integrity of video data transferred from source to destination. Security Alert Algorithm ensures authentication for rejecting the malicious nodes from being intermediate nodes, which is to be discussed in Section V.

To accomplish the second objective, i.e., controlling high bandwidth consumption, the following strategy is adopted in the proposed work.

The video frames in the SVC (Scalable Video Coding) technique, are split into base layers for having basic video information and enhancement layers for refinement of video data. Before using encryption technique, the all the base layers and only a few enhancement layers are compressed to achieve low bandwidth consumption that is very much required performance metric for video streaming applications in MANET.

To fulfill the third objective, i.e., achieving reliable video streaming without causing errors and loss of data, a reliable multipath propagation of compressed and encrypted video data, is carried out

C. Topological Design

These three objectives can be accomplished in the non-overlapping zone routing network topology that is classified into Intra and Inter routing zones as shown in Fig. 2. The entire region of the networking topology has been divided into different non-overlapping zones so that the communications between nodes in a zone are established by Intra-zone routing and the communications between nodes of different zones are established through BRNs which are deployed on the border of each zone by Inter-zone routing. The BRNs are deployed with powerful Directional Antennas (DAs) so as to ensure confidentiality, integrity, and authenticity, and propagate the signals effectively among the BRNs of the neighboring zones ensuring the identity of the nodes in their respective coverage region by recording in the authenticated nodes of Intra zones using two-hop communication.

D. Parameter Analysis

The parameters such as security, bandwidth and reliability have been analyzed thoroughly to establish the video streaming in MANET. From the analysis, it is observed that these parameters need to be improved for effective video streaming in MANET. The performances of the video streaming application can be enhanced by improving these parameters by suitably incorporating certain strategies in the proposed work with which the problems of high bandwidth consumption, security problems and unreliability can amicably be solved. The solutions to improve these parameters are discussed as follows.

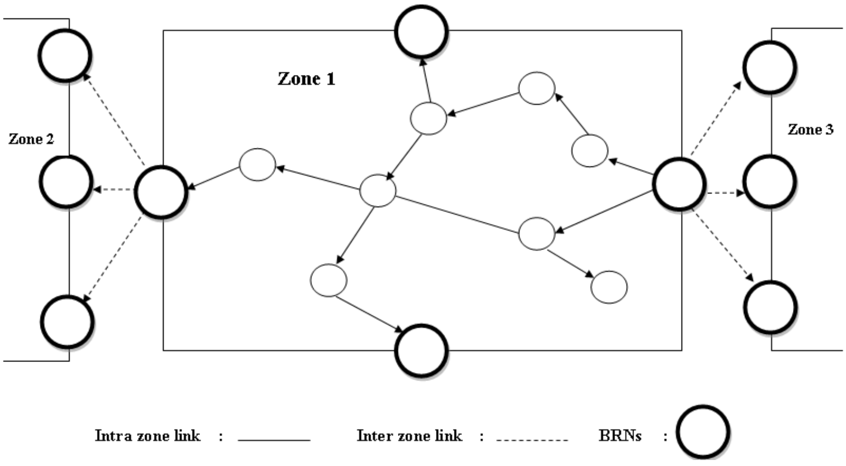

Fig. 2 Intra and Inter zones communication

E. Solution for Security Problems

The layered coding based video packets are encrypted and propagated from source to destination using symmetric key encryption technique among the members of Intra-zone and BRNs of Inter zones. The symmetric key encryption technique along with a highly secure instant session key through public key double encryption technique ensures confidentiality and integrity without imposing any overhead such as computationally intensive and memory intensive operations so that it can be appropriate for streaming applications in MANET. Nonetheless, the only problem with the symmetric key encryption technique is to maintain the privacy of the shared secret key between the source and destination.

To solve the problem of maintaining the privacy of the shared secret key, an instant session key which is only known to sender and receiver, is generated with highly secure public key double encryption technique and transmitted from source to destination. Then, all encrypted video packets in the destination are decrypted with the instant session key. A Security Alert Mechanism is triggered by BRNs to authenticate the nodes and reject the malicious nodes from being intermediate nodes as an authentication procedure.

The proposed work, therefore, offers double protection in terms of confidentiality, integrity and authentication by incorporating symmetric key encryption technique in streaming the video packets from source to destination and adopting the highly secure public key double encryption technique in the instant session key generation for sharing the secret key between source and destination at the end of every propagation of encrypted video packets transmitted from source to destination through the nodes in the Intra zones and BRNs in the Inter zones along with authentication.

F. Solution for High Bandwidth Consumption

The problem of high bandwidth consumption is addressed by Secure Low Bandwidth (SLB) Video Streaming Algorithm. A scalable representation of video signals consists of few base layers and multiple enhancement layers. The base layer provides an essential level of quality and can be decoded independently of the enhancement layers. On the other hand, the enhancement layers serve only to refine the base layer quality. Therefore, the base layers that represent the most critical part of the scalable representation, are used to make the performance of streaming applications effective. So they are encrypted with compression but only the selective enhancement layers out of multiple layers are picked up for compression and are encrypted using the symmetric key algorithm. The compressed and encrypted video data in the source node are transmitted through secure multi-paths of Intra and Inter zones to the destination node where the decryption and decompression are performed, and base layers and selective enhancement layers, are reconstructed to retrieve the original video sequence using the Motion Compensation technique [11] and Frame Replenishment technique [12] which are to be discussed in the Section III.

G.Solution for Unreliability

The problem of unreliability is addressed by propagating the video packets through Multi-paths which are selected by Reliable Secure Multipath (RSM) Propagation algorithm so that the number of packets forwarded from source to destination is according to the priority that is, the paths of less discovery time and high-Security Index Ratio (to be discussed in the Section V), will tend to transmit more number of packets.

The methodologies implemented by the proposed system for solving the problems of high-bandwidth consumption, insecurity, and unreliability in the video streaming applications of MANETs, are elucidated in the Sections III, IV, and V respectively.

Open Science Index, Computer and Information Engineering Vol:9, No:6, 2015 publications.waset.org/10002105.pdf

Open Science Index, Computer and Information Engineering Vol:9, No:6, 2015 publications.waset.org/10002105.pdf

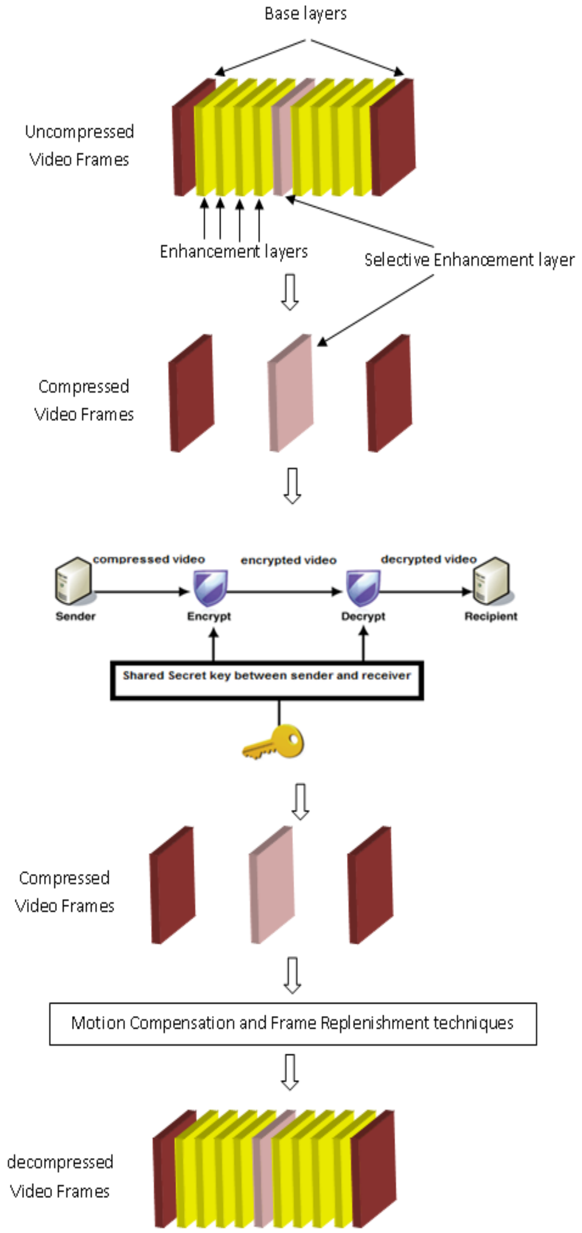
Base layers
Uncompressed Video Frames
Enhancement layers
Selective Enhancement layer
Compressed Video Frames
compressed video
encrypted video
decrypted video
Sender
Encrypt
Decrypt
Recipient
Shared Secret key between sender and receiver
Compressed Video Frames
Motion Compensation and Frame Replenishment techniques
decompressed Video Frames

Fig. 3 Sequence of processing video frames

II. Related Works

A few research papers have dealt the security issues in ad hoc networks: The security issues particularly in ad-hoc networks have been addressed by including key management [13], secure routing protocols [14], handling node misbehavior [15] and preventing traffic analysis [16]. The data confidentiality service in an ad hoc network is the protection of data from passive attacks like eavesdropping while they are transmitted across the network. The wireless channel in a hostile environment is vulnerable to various forms of attacks, particularly the eavesdropping. The other single path security mechanisms avoid misbehavior on routing and data transmission in ad hoc networks have been presented by various authors [16]-[18]. A robust multipath delivery is elucidated in [19] for improving the resilience of the transmitted packets through multipath propagation. In MANET, the routing protocols such as Dynamic Source Routing (DSR) [20] and Ad-hoc On-demand Distance Vector (AODV) [21] can be used. However, the unreliability of the wireless medium, the dynamic topology due to nodes mobility, frequent communication failures and high delays for path reestablishments have been reported from them. So a multi-path routing is a very promising alternative to single path routing as it provides higher resilience to path breaks and alleviates network congestion through load balancing and reduces end-to-end delay [22]. Thus, the multi-path routing can be highly suitable for multimedia streaming over wireless ad hoc networks. Nonetheless, as security remains an important issue that hinders the rapid deployment of multimedia applications over wireless ad hoc networks, security issue must be addressed in multi-path multimedia streaming over wireless ad hoc networks [23]. Lou et al. have presented a scheme called Security Protocol for Reliable data Delivery (SPREAD) in [24], which provides further protection to then existing data confidentiality service in an ad-hoc network using multipath routing. It aims at the protection of secret messages from being revealed. A secret message is transformed into multiple shares using the threshold secret sharing algorithm, are delivered via multiple node-disjoint paths to the destination. As the shares are delivered through multiple node-disjoint paths, barring a few number of shares, the secret message as a whole cannot be compromised. However, as it is necessary for all the paths to deliver at least one share, the natural parallel redundancy of the multiple paths is reduced to serial redundancy and therefore, a malicious node dropping all packets or a broken link may disrupt the protocol. Moreover, SPREAD is not suitable for multimedia streaming, as it is not meant for real-time data transfer [24]. Mavropodi et al have proposed an on-demand multipath routing protocol called Secure Multipath Routing (Sec-MR) protocol [25] that can find multiple node disjoint routes with protection against Denial-Of-Service (DoS) attacks from a bounded number of collaborating insider attackers. However, the authors have mentioned that Sec-MR protocol does not fully protect from Man-In-Middle (MIM) and invisible node attacks.

From the survey, we have observed that there is no currently existing protocol that suitably gets adapted to video streaming applications in MANET with enhanced security aspects and reliability along with low bandwidth consumption.

A. Motivation

The driving problems such as lack of security aspects, high bandwidth consumption and unreliable video transmission in the mobile ad hoc video streaming applications, have been addressed by the proposed architecture Secure Low-bandwidth Video Streaming through Reliable Multipath Propagation (SLVRMP). The primary security aspects with reduced bandwidth consumption and improved reliability can be achieved through Secure Low Bandwidth (SLB) Video Streaming Algorithm and Reliable Secure Multipath (RSM) Propagation Algorithm respectively using Layered Video Coding in non-overlapping zone routing network topology.

Open Science Index, Computer and Information Engineering Vol:9, No:6, 2015 publications.waset.org/10002105.pdf

III. Design of the Proposed System

Video data requires an enormous amount of storage and bandwidth capacity. The bandwidth of a network describes the maximum data transfer rate of the network. It measures how much data can be sent over a specific channel within a stipulated time. It does not measure how fast bits of data move from one point to another. Instead, it measures how much data can flow through a specific channel at one time. Continuous data, especially in the form of real-time communications (e.g., audio/video-conferencing) would be impossible, as nature of the real-time transmission of video data would put enormous strain even on high-speed fiber optic networks. To facilitate a feasible and less bandwidth consuming real-time communication over MANETs, data are usually compressed to a fraction of space/bandwidth requirements of its uncompressed form.

The Scalable Video Coding (SVC) standard as an extension of H.264/AVC [26] provides an efficient, standard based scalability of temporal, spatial, and quality resolution of a decoded video signal. The goal of the Layered Coding is to create dependent layers, i.e., one base layer and several enhancement layers that can be used, one after another, to refine the decoded quality of the base layer. An important feature of SVC is that enhancement layers can be dropped any time while the base layer must never be dropped off. If the base layer is not received, nothing can be enhanced by the successive layers. Layered Coding is designed to obtain such a kind of scalability.

Using the aforementioned important feature of SVC standard, all the base layers, and the selective enhancement layers are compressed and encrypted so that the bandwidth and security of the network can be greatly improved. Fig. 3 shows the sequence of processing of base and enhancement layers using compression and encryption techniques incorporated in the proposed system

The problem of high bandwidth consumption of video packets can be addressed effectively by compressing the selective enhancement layers of the video data after discarding similar and redundant successive frames and compressing all the base layers. It greatly reduces the bandwidth consumption of video data and enhances the data transmission rate of the video streaming using Frame Replenishment and Motion Compensation techniques.

In Frame Replenishment technique, not all the pixels in every frame are coded. However, only changing pixels are encoded for every frame, and unchanging pixels for a set of frames are coded only once and just repeated over the next frames.

In Motion Compensation technique, a method called displacement based predictive coding is used in which the changes between the successive frames are considered due to the translation of moving objects in the planes of the video frame.

The video data is segregated into two different layers of video frames namely base layers and enhancement layers. Only the frames of base layers that have distinct and independent features are selected for encryption, and the most of the enhancement layers that have almost similar and dependent features are discarded because of their redundancy. Only selected enhancement layers that have abrupt changes are selected for encryption and rest of the layers are discarded so that the keyframes and enhancement frames in the destination can be used to build the entire video sequence after decryption as shown in Fig. 3.

The Base and Enhancement layered video frames are duplicated in view of achieving the reliability in receiving the frames intact at the destination.

A. Comprehensive Security Model

The primary security aspects viz., confidentiality, integrity, and authentication are established in the non-overlapping zone routing network. The proposed comprehensive security model has been established in two phases.

In the first security phase, the layered coding based video packets are compressed and encrypted to propagate it from source to destination through Secure Multipath Propagation using shared secret key S_k with symmetric key encryption technique as shown in Fig. 4.

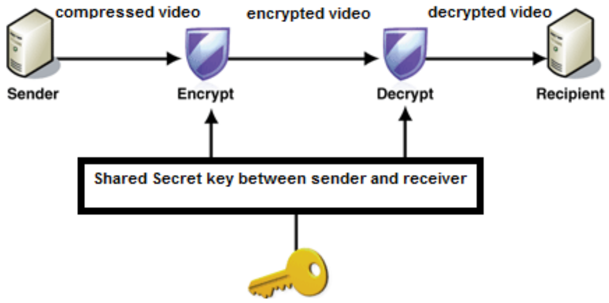

Fig. 4 Symmetric key encryption technique

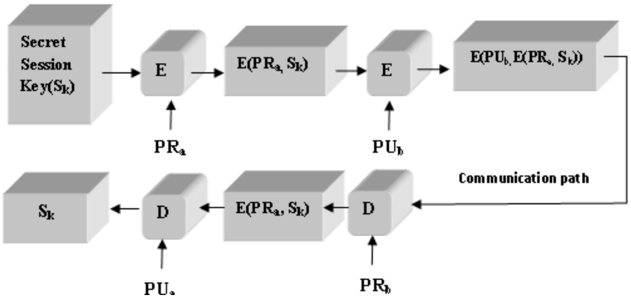

Fig. 5 Public key double encryption technique

In the second security phase, an instant session key which is only known to sender and receiver is generated during propagation with public key double encryption technique and transmitted from source to destination to decrypt the previously received compressed video packets in the destination as shown in Fig. 5.

B. SLB Video Streaming Algorithm

The processing steps of SLB Video Streaming Algorithm for incorporating compression and encryption techniques in the proposed system are as follows:

Step 1. All base layers are selected for compression

Open Science Index, Computer and Information Engineering Vol:9, No:6, 2015 publications.waset.org/10002105.pdf

Step 2. The selected enhancement layers of video data which have abrupt changes, are selected for compression

Step 3. The selected base and enhancement layered frames are duplicated to enhance the reliability

Step 4. Base layers are compressed and duplicated as BLCompression-duplication {BL1,BL1, BL2,BL2, BL3,BL3 ... BLn,BLn} using Replenishment technique

Step 5. Enhancement layers are compressed and duplicated as ELCompression-duplication {EL1,EL1, EL2,EL2, EL3,EL3 ... ELn,ELn } using Motion compensation technique

Step 6. The compressed video packets are encrypted as E(BLCompression || ELCompression, S_k(Sessionkey)) using symmetric key encryption

Step 7. The compressed and encrypted video packets are transmitted from the source node to target node using Reliable Multipath Propagation algorithm that is to be discussed in Section IV.

Steps 1-7 are iteratively carried out at the start of every reliable multipath propagation till the end of the video session.

IV. Reliable Multipath Propagation

A. Route Discovery Phase

The route discovery phase of the proposed system is divided into two phases namely Intra-zone discovery phase and Inter-zone discovery phase in which proactive OLSR [27] and reactive ODMRP [28] protocols are implemented respectively over non-overlapping zones. The entire network has been segregated into a number of non-overlapping zones whose boundaries are placed with super hosts called BRNs deployed by powerful DAs. The BRNs which are arbitrarily placed on the boundary line of each zone, communicate with the BRNs of other zones. The inter-zone communication is facilitated using beam forming DAs implemented through the Multi-hop RTS MAC (M-MAC) protocol in data link layer. The OLSR is implemented in the Intra zones to adopt an effective communication with low overhead among the nodes within a zone.

The processing steps involved in the Intra and Inter-zone discovery phases in the proposed system are as follow:

BRNs are the nodes that are placed arbitrarily on the boundary of each zone, and they transmit the video data to other BRNs of the nearby/adjacent zones with the help of the deployed DAs for two-hop distance.

When the source node has data to send to the destination node, first it checks the address of the destination node in its route cache. If the address of target node is found in its cache, the process of discovery is over and immediately the video data is transmitted through SLB Video Streaming Algorithm using OLSR to the target that is present in the intra-zone.

If the destination node is not found in its route cache, it sends a route request to its neighboring BRN which stores the addresses of the BRNs of the same and neighboring zones. If the destination node is found in the BRNs of the source zone, the data is transmitted to the destination using OLSR protocol otherwise the Inter-zone routing discovery is initiated by sending the route requests to the BRNs of neighboring zone.

If the target node is not found within the intra-zone, the discovery process of finding the target node in the inter-zone is now carried out only by forwarding the route requests to other neighboring BRNs on the boundary of adjacent zones with ODMRP. It forms a multicast forwarding Group that is effectively used to find the destination node without control overhead.

The discovery time can be calculated with time-based distance measure method by synchronizing clocks in source and destination and recording Time of Flight (ToF) of a signal from the source to destination. The Security Index Ratio can be calculated by calculating the ratio of a number of packets successfully reaches the destination per number of packets transmitted through that path from the source.

The nearby BRNs that receive the route request resume the process of finding the target node in their respective zone recursively. If the destination is found, immediately the route reply is passed over to its preceding BRNs in the reverse path one by one and finally reaches the source node.

The flow diagram of the processing involved in the Secure Reliable Multipath propagation is shown in Fig. 6.

The processing steps involved in the Reliable multipath propagation are as follows:

Step 1. Source node S transmits the video data after compression and encryption to a nearby BRN_{ij} of its zone where i represents zone ID, and j represents BRN ID (ex: BRN_{11} represents the BRN of ID1 in the Zone1).

Step 2. BRN_{ij} transmits the compressed and encrypted video data to other BRNs of the same zone.

Step 3. Each BRN of the zone that receives video data, forwards them through Secure Reliable Multipath propagation algorithm with the multi-paths of minimum discovery time and high-Security Index Ratio calculated during the route discovery phase using ODMRP.

Step 4. The compressed and encrypted video data are forwarded through members of multicast group which form the prioritized paths of the selected BRNs on the basis of minimum discovery time with high Security Index Ratio to destination through Forward Multicast Group. The number of the packets that are sent through the prioritized paths is directly proportional to discovery time and Security Index Ratio from source to destination. *The lesser the discovery time and the higher Security Index, the more packets are transmitted through the prioritized path.*

Step 5. The target BRN, which is nearer to the target node, receives the compressed and encrypted video data from the rest of the BRNs of the target zone.

Step 6. The video packets collected from the BRNs of the target zone are forwarded to the target node by the target BRN which is nearer to the target node using OLSR where the processes of decompression and decryption are performed.

Open Science Index, Computer and Information Engineering Vol:9, No:6, 2015 publications.waset.org/10002105.pdf

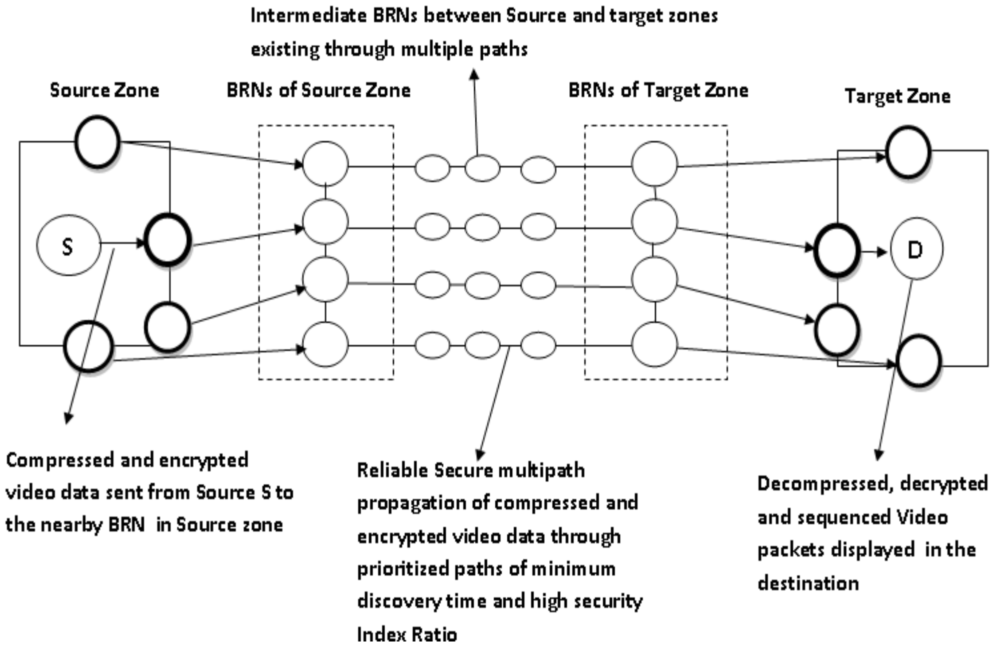
Intermediate BRNs between Source and target zones existing through multiple paths
Source Zone
BRNs of Source Zone
BRNs of Target Zone
Target Zone
S
D
Compressed and encrypted video data sent from Source S to the nearby BRN in Source zone
Reliable Secure multipath propagation of compressed and encrypted video data through prioritized paths of minimum discovery time and high security Index Ratio
Decompressed, decrypted and sequenced Video packets displayed in the destination

Fig. 6 Flow Diagram of Secure Reliable Multipath Propagation

V. Security Management System

A new performance metric called Security Index Ratio (SIR) is included for evaluating the level of security in the proposed system and it is defined as the ratio of number of video packets safely received in the destination through one of the multi-paths to the total of number of packets transmitted through that path from the source BRN to the target BRN.

This parameter can be better illustrated with an example. Let the number of packets sent from the source to destination be $NoP_{tot.}$ Let the number of packets safely recovered at destination after successful decompression and decryption be NosP, then:

$$SIR = \mathrm{NosP} / \mathrm{NoP}_{tot}$$

where NosP packets successfully received at the destination through one of the multi-paths after successful decompression and decryption; and NoP_{tot} number of packets sent from the source to destination through the same path.

It indicates that the amount of safely recovered video packets after every propagation without causing any packet dropping in transition either by congestion or security threat.

The packets dropping may be caused either by congestion or by the vulnerability. The importance of the parameter is that if it drastically gets reduced, it is the indication of sudden congestion or vulnerability. In that case, all the BRNs of the concerned path are thoroughly checked out for finding the reason for the sudden packets dropping. In the analysis, if it is observed that the dropping is due to congestion, then the number of packets transmitted are reduced by congestion control mechanism or if it is observed that the dropping is due to some malicious node, then immediately the path is abandoned and all the BRNs along the path are revoked and alerted of finding the malicious nodes and rejecting them from being intermediate nodes to the propagation of video packets to destination.

Then, there a question arises as to how to distinguish the packet dropping due to congestion from packet dropping due to malicious nodes. The solution is to find the Security Ratio Offset value that is the difference of the Security Index Ratios of two consecutive propagations through a multipath. If Security Ratio Offset is greater than 50%, propagation through the path is abandoned, and Security Alert Mechanism of the BRNs in the path is triggered out. If the congestion is due to malicious nodes, all the BRNs in the path are revoked otherwise the next propagation is carried out after implementing congestion control mechanism of reducing 25% of the previously transmitted packets through the path.

Thus, secure multi-paths are established by constantly observing the Secure Index Ratio parameter. Security Alert Mechanism for the BRNs is triggered for the path whose Secure Ratio Offset is greater than 50%. The value 50% is not a rigid ratio number with which Secure Ratio Offset is set. The value may be varying depending upon the applications in which it is being used. Here in case of video streaming in MANET, it has been fixed as 50% but it may differ from application to application depending on the propagation scenario.

The flow diagram for finding the Security Ratio Offset and implementing Security Alert Mechanism and Congestion Control Mechanism is shown in Fig. 7.

Open Science Index, Computer and Information Engineering Vol:9, No:6, 2015 publications.waset.org/10002105.pdf

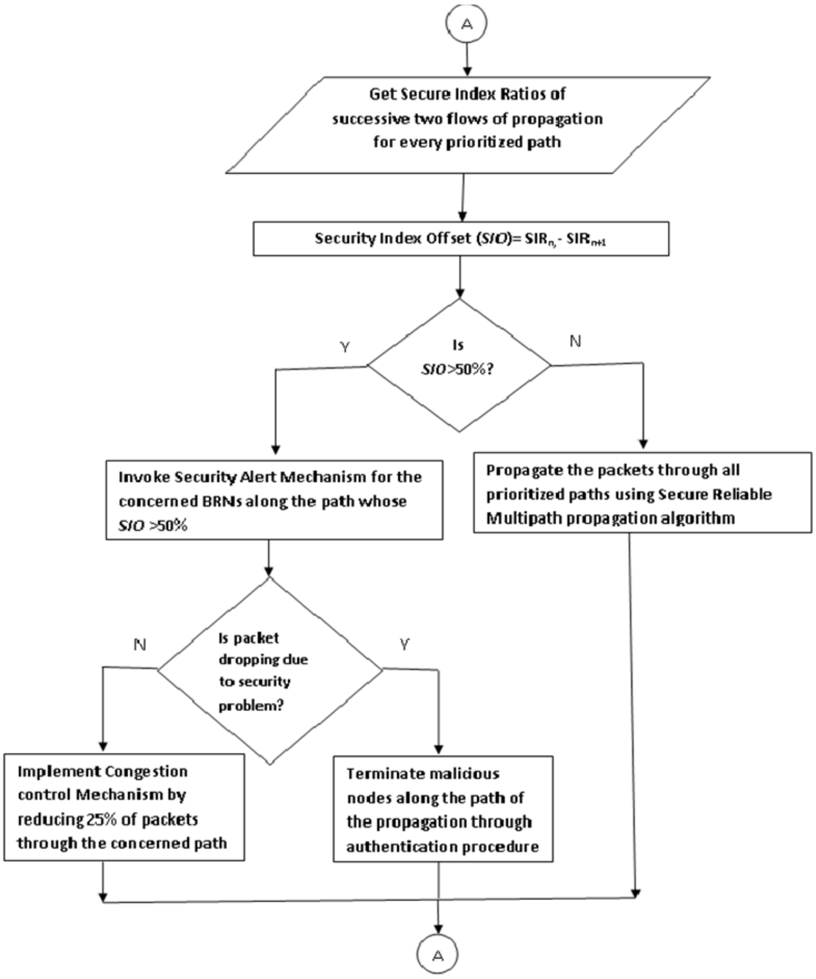
A
Get Secure Index Ratios of successive two flows of propagation for every prioritized path
Security Index Offset (SIO)= SIR$_n$ - SIR$_{n+1}$
Y
Is SIO>50%?
N
Invoke Security Alert Mechanism for the concerned BRNs along the path whose SIO >50%
Propagate the packets through all prioritized paths using Secure Reliable Multipath propagation algorithm
N
Is packet dropping due to security problem?
Y
Implement Congestion control Mechanism by reducing 25% of packets through the concerned path
Terminate malicious nodes along the path of the propagation through authentication procedure
A

Fig. 7 Flow Diagram for Invoking Security Alert and Congestion Control Mechanisms

A. Secure Data Transmission Phase

After establishing the route from the source to the destination in the route discovery phase, the data that are to be transmitted, are forwarded through members of multicast group so that the security of the system can be greatly enhanced. As a result of route establishment to the destination, it is possible that there are different flows between the source BRN and target BRN. Only the paths of the selected BRNs of a multicast group that is of minimum discovery time to reach destination and high-Security Index Ratio are involved in the secure data transmission phase. High-Security Index Ratio prioritizes the paths with minimum discovery time. Therefore, the path with high-Security Index Ratio and minimum discovery time is selected first. Similarly subsequent routes to the destination are selected to forward data packets from source BRNs to destination BRNs on a priority basis of high-Security Index Ratio with minimum discovery time. The number of packets which can be forwarded through every selected disjoint path from source BRNs to destination BRNs can be calculated as follows.

If there are p1, p2, and p3 prioritized paths from source to destination, then the set P = {p1, p2 and p3} is selected to route data packets from source BRNs to destination BRNs.

The number of packets which can be forwarded from source BRNs to destination BRNs through disjoint paths can be calculated as follow

The LCM for the Security Index Ratio of paths, L1, L2, L3 is found to be L and ratio of number of packets between the paths can be calculated as the ratio of packets which can be routed among the paths p1,p2, and p3 can be calculated as L/L1: L/L2: L/L3.

Let N be the total number of packets that need to be routed from source to destination.

Let the source BRN and destination BRN be SBRN and DBRN respectively.

No of packets which can be routed through p1 = L/L1*N
No of packets which can be routed through p2 = L/L2*N
No of packets which can be routed through p3 = L/L3*N

B. Secure Reliable Multipath Propagation Algorithm

Step 1. Get the different flow paths from source BRNs to target BRNs from Route Discovery Phase as input paths.

Step 2. Compare different flow paths in terms of the Security Index Ratio and Discovery Times. The path with high-Security Index Ratio and Minimum Discovery Time to reach destination, is selected as the first priority, and

Open Science Index, Computer and Information Engineering Vol:9, No:6, 2015 publications.waset.org/10002105.pdf

the process is carried out till all flows of path are prioritized.

Step 3. Find the LCM for Security Index Ratio of first 3 selected paths L1, L2, and L3 (i.e., L).

Step 4. Find the ratio of the packets that can be routed L/L1: L/L2: L/L3.

Step 5. Route the packets from SBRN to DBRN as L/L1* N, L/L2*N, L/L3*N.

Step 6. Iterate the Step 1 through Step 5 for every secure data transmission phase.

The above logic of the SRM propagation algorithm can be illustrated with a simple example. Let us assume that a total video data of 1500 packets needs to be routed from an SBRN to a DBRN. The Route Discovery algorithm is implemented to find a set of paths with high-Security Index Ratio and minimum route discovery time. Let us consider that the algorithm finds five disjoint paths p1, p2, p3, p4, p5 having route discovery time 60 ms, 200 ms, 120 ms, 230 ms, and 180 ms respectively between SBRNs to DBRNs. These paths are assumed to have 90%, 60%, 75%, 55% and 60% Security Index Ratios respectively. The high-Security Index Ratio with minimum discovery time is selected first. Therefore, the path set P={p1, p3, and p5} is selected to route data packets from SBRNs to DBRNs. The number of packets which can be forwarded from SBRNs to DBRNs through disjoint paths can be calculated as 90:75:60 = 6:5:4. The LCM of 6, 5,4 is 60 and the ratio of packets that can be routed among the paths p1,p3and p5 can be calculated as 6:5:4. The sum of all the parts is 6+5+4 =15.

No of packets which can be routed through the path P1= 6 * 1500/15 = 600 packets

No of packets which can be routed through the path P3= 5* 1500/15= 500 packets

No of packets which can be routed through the path P5= 4* 1500/15= 400 packets

From the above algorithm, the number of packets forwarded to source to destination is according to the priority that is, the paths with high-Security Index Ratio and less discovery time will tend to transmit more number of packets through secure path.

The secure multi-path propagation algorithm transmits the remaining of video packets from other SBRNs to DBRNs in some iterations similarly the way described earlier till all the packets are sent from source to destination on the priority of high-Security Index Ratio and less discovery time using ODMRP through Forward Multicast Group.

VI. Advantages of the Proposed System

The proposed system offers the following advantages:

1) The problem of high bandwidth consumption of voluminous video packets can effectively be addressed by compressing the selective enhancement layers of the video data after discarding similar and redundant successive frames using Motion Compensation technique and compressing all the base layers using Frame Replenishment technique.
2) A comprehensive security model is established to maintain primary security aspects such as confidentiality and integrity by adopting the encryption of video frames by shared secret key S_k using symmetric key encryption technique at every propagation in the first security phase and public key double encryption technique is implemented for sharing the shared secret key between source and destination in the second security phase.
3) The performance of the video streaming in terms of authentication service gets considerably improved with the deployment of BRNs in the boundary of non-overlapping zones to route the video packets towards destination by rejecting malicious nodes from being intermediate nodes in the propagation of video packets to destination through ODMRP using DAs.
4) The video frames in the form of base and enhancement layers that are compressed and forwarded through different BRNs of non-overlapping zones in multi-paths consume very less bandwidth compared to those of other protocols in video streaming applications.
5) The BRNs of non-overlapping zones used in the proposed system are flexible in the data transmission and the BRNs of the each zone act as decentralized cluster heads and are reliable even if any one of the BRNs fails to work.
6) The reliability of the system gets greatly improved as the video data are sent through multi-paths in which video frames in the form of base and enhancement layers are transmitted with duplication.

VII. Simulation Results and Implications

Secure Low Bandwidth Video streaming through Reliable Multipath Propagation (SLVRMP) protocol architecture has been proposed by incorporating the two algorithms namely Secure Low Bandwidth (SLB) Video Streaming Algorithm and Reliable Secure Multipath (RSM) Propagation Algorithm using Layered Video Coding in non-overlapping zone routing network topology. The performances of the proposed system are compared to those of the other existing secure multipath protocols Sec-MR [27], SPREAD [26] using NS 2.34 and the simulation results show that the performances of the proposed system get considerably improved.

A. Simulation Environment

The parameters of communication model are shown in Table I. The performances of the proposed SLVRMP protocol architecture are compared to the existing Secure Multipath protocols Sec-MR and SPREAD with key performance metrics such as Bandwidth, Security Index Ratio and Packet dropping using Network Simulator 2.34(ns 2.34) and the results are shown in Tables II-IV and Figs. 8-10.

B. Performance Metrics

The following metrics are used in this work for the performance analysis of the proposed SLVRMP with Sec-MR and SPREAD multipath routing protocols.

i. Bandwidth
ii. Security Index Ratio
iii. Packet dropping

Open Science Index, Computer and Information Engineering Vol:9, No:6, 2015 publications.waset.org/10002105.pdf

TABLE I
PARAMETERS OF COMMUNICATION MODEL

Parameter	Value
Simulator	NS-2.34
Simulation Time	500 Seconds
Area-of-Network	750 m x 750 m
No of Nodes	200
Mobility Model	Random Waypoint
Pause Time	25, 50,75, 100, 125, 150, 175, 200 s
Traffic	CBR (Constant Bit Rate)
Transmission Range	250 m
Node Speed	fixed to 20 m/s

C. Bandwidth

It describes the maximum data transfer rate of a network and measures how much data can be sent over a specific connection in a given amount of time. The general unit for measuring bandwidth is Mbps (Megabits per second). As video data are voluminous in nature, it is very important to consider these metrics to evaluate the performance of the network.

D. Security Index Ratio

It is the ratio of a number of video packets safely received in the destination through one of the multi-paths to the total of the number of packets transmitted through that path from the source to destination. The metric *SIR* is used to visualize how much data can reach the destination safely without packet dropping either due to security threat or congestion in the network. It is an important metric as it is an indication of secure data transfer in video streaming applications.

E. Packet Dropping

It is a performance metric that directly indicates how much amount of data is lost in the transmission that may be due to security threat or due to congestion in the network. It is an important metric to evaluate security threat or congestion in the network. The performance of *SIR* can be improved by reducing packet dropping in the network.

The performance of Bandwidth in the proposed system is shown by plotting Bandwidth with respect to Number of Secure and Reliable paths in Table II and Fig. 8.

TABLE II
BANDWIDTH VS. NO OF SECURE AND RELIABLE PATHS FOR SEC-MR, SPREAD, AND THE PROPOSED SLVRMP PROTOCOLS

No of Secure and Reliable Paths	Bandwidth (MB)		
	SPREAD	Sec-MR	Proposed SLVRMP
5	950	820	720
10	900	770	670
15	850	710	610
20	800	660	530
25	740	600	450
30	590	500	360
35	490	410	260
40	390	300	150
45	280	230	100
50	170	120	50

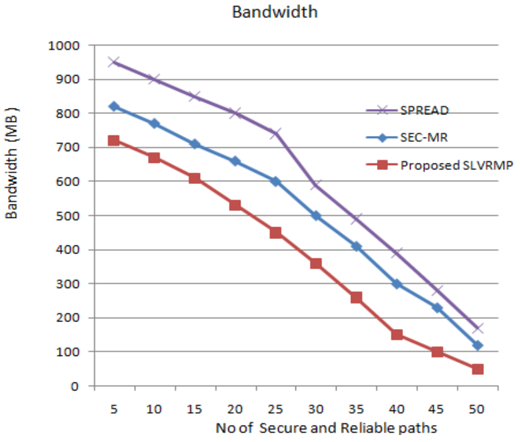

Fig. 8 Bandwidth vs. No of secure and reliable paths for Sec-MR, SPREAD and proposed SLVRMP protocols (Number of nodes = 200, area space = 750 m x 750 m)

TABLE III
SIR VS. NO OF SECURE AND RELIABLE PATHS FOR SEC-MR, SPREAD, AND PROPOSED SLVRMP PROTOCOLS

No of Secure and Reliable Paths	Security Index Ratio		
	SPREAD	Sec-MR	proposed SLVRMP
0	0.4	0.4	0.4
25	0.44	0.46	0.42
50	0.5	0.49	0.46
75	0.52	0.52	0.47
100	0.54	0.53	0.48
125	0.59	0.57	0.49
150	0.63	0.58	0.51
175	0.69	0.6	0.53
200	0.72	0.62	0.55

The performance of Security Index Ratio in the proposed system is shown by plotting Security Index Ratio with respect to No of Secure and Reliable paths in Table III and Fig. 9.

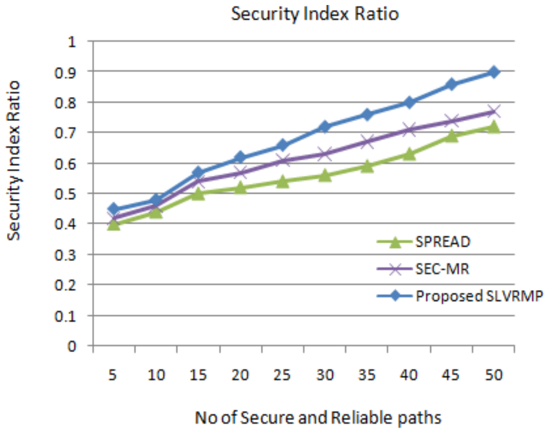

Fig. 9 *SIR* vs. No of secure and reliable paths for Sec-MR, SPREAD, and proposed SLVRMP protocols (number of nodes = 200, area space = 750 m x 750 m)

The simulation result shown in Fig. 8 implies that the average performance of Bandwidth gets considerably improved by 37.94% in the proposed system when compared

Open Science Index, Computer and Information Engineering Vol:9, No:6, 2015 publications.waset.org/10002105.pdf

to the average performances of Sec-MR and SPREAD as video data are transmitted from source to destination after compression of base and enhancement layers through multiple paths using the proposed SLB Video Streaming Algorithm as explained in Section III.

The simulation result shown in Fig. 9 implies that the average performance of *SIR* gets moderately improved by 13.37 % in the proposed system when compared to the average performances of Sec-MR and SPREAD as video data are transmitted from source to destination by suitable triggering Security Alert Mechanism or Congestion Control Mechanism and selecting secure and reliable paths using the proposed RSM Propagation Algorithm as explained earlier.

The performance of Packet dropping in the proposed system is shown by plotting Packet dropping with respect to No of Secure and Reliable paths in Table IV and Fig. 10.

TABLE IV
PACKET DROPPING VS. NO OF SECURE AND RELIABLE PATHS FOR SEC-MR, SPREAD AND PROPOSED SLVRMP PROTOCOLS

No of Secure and Reliable Paths	Packet dropping		
	SPREAD	Sec-MR	proposed SLVRMP
0	0.4	0.4	0.4
25	0.44	0.46	0.42
50	0.5	0.49	0.46
75	0.52	0.52	0.47
100	0.54	0.53	0.48
125	0.59	0.57	0.49
150	0.63	0.58	0.51
175	0.69	0.6	0.53
200	0.72	0.62	0.55

The simulation result shown in Fig. 10 implies that the average of Packet dropping gets considerably reduced by 33.38 % in the proposed system when compared to the average performances of Sec-MR and SPREAD as video data are transmitted from source to destination by suitable triggering Security Alert Mechanism and selecting secure and reliable paths using the proposed Reliable Secure Multipath Propagation Algorithm as discussed earlier.

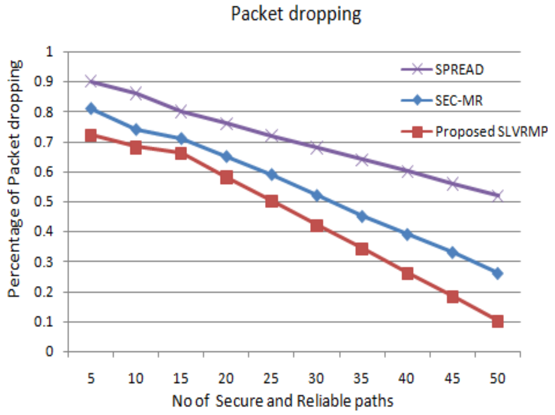

Fig. 10 Packet dropping vs. No of secure and reliable paths for Sec-MR, SPREAD, and proposed SLVRMP protocols (number of nodes = 200, area space = 750 m x 750 m)

VIII. CONCLUSION

We have presented a non-overlapping Zone based secure, low bandwidth consuming and reliable Multipath Routing architecture specially designed for improving the parameters reliability, bandwidth and security of video streaming in Mobile Ad hoc network. It is a reliable security architecture which transmits the video data to destination through symmetric private key encryption technique and shares the symmetric session key through public key double encryption technique so as to ensure the primary security aspects authentication, confidentiality and integrity. The combined strategy of compression and encryption considerably improves security, bandwidth, and reliability through Reliable Secure Multipath Propagation Algorithm and Secure Low-bandwidth Video Streaming Algorithm by adopting multipath route discovery procedure. The simulation results show that Bandwidth, *SIR* and Packet dropping get improved by 37.94%, 13.37% and 33.38 % respectively in the proposed system when compared to those of the Sec-MR and SPREAD Multipath protocols and the implications of the result have been already discussed in the simulation results of Section VII itself.

Though the simulation results show signs of improvement in the parameters Bandwidth, *SIR* and Packet dropping, the parameters such as scalability, mobility, energy-efficiency, and link stability are not considered in this work. These parameters need to be analyzed in perspective of video streaming applications over Mobile ad hoc networks by incorporating appropriate enhancements in the proposed work as a future scope of research work.

REFERENCES

[1] M. Lindeberg, S. Kristiansen, T. Plagemann and V. Goebel, “Challenges and Techniques for Video Streaming over Mobile Ad Hoc Networks,” Multimedia Systems, Volume 17, Number 1, pp.51-82, Springer – Verlag, 2011.

[2] Tim Bohrloch, Carlos T. Calafate, A. Torres, J. C. Cano and P.Manzoni, “Evaluating Video Streaming Performance in MANETs Using a Testbed,” XXII Jornadas de Paralelismo Sept 2011.

[3] C. Y. Tseng, P. Bala Subramanyam, and C. Ko, et al., “A Specification-Based Intrusion Detection System for AODV,” in Proc. of ACM Workshop on Security of Ad Hoc and Sensor Networks, VA, 2003, pp. 125–134.

[4] A. Boukerch, L. Xu, and K. EL-Khatib, “Trust-Based Security for Wireless Ad Hoc and Sensor Networks,” Computer Communications 30 (2007) 2413–2427.

[5] D. Djenouri, L. Khelladi, and N. Badache, “A Survey of Security Issue in Mobile Ad Hoc and Sensor Networks,” IEEE Communications Surveys & Tutorials 7 (2005) 2–28.

[6] Wei Wang, Huiran Wang, Beizhan Wang, Yaping Wang, and Jiajun Wang, “Energy-Aware and Self-Adaptive Anomaly Detection Scheme Based on Network Tomography in Mobile Ad Hoc Networks,” Elsevier-Information Sciences 220 (2013) 580–602.

[7] H. Yang, G. Zhong, and S. W. Lu, “Network Performance Centric Security Design in MANET,” ACM Mobile Computing and Communications Review 6 (2002) 121–130.

[8] Zheng Wan, “Adaptive Video Transmission in Manets,” Proceedings of IC-BNMT 2009.

[9] Harsharndeep Singh, MeenuDhiman and HarmunishTaneja “EVSM: Enhanced Video Streaming in Mobile Ad-Hoc Networks,” International Journal of Computer Science and Telecommunications, Volume 3, Issue 9, September 2012.

[10] Haas, Z.J., and Pearlman, M.R., “The performance of query control schemes for the zone routing protocol,” IEEE/ACM Trans. Netw, 9(4), 427–438, 2001.

[11] JiefuZhai, Keman Yu, Jiang Li, and Shipeng Li “A Low Complexity Motion Compensated Frame Interpolation Method,” ISCAS 2005, May 2005.

[12] Y.J. Chiu and T. Berger, “A software-only video codec using pixel wise conditional differential replenishment and perceptual enhancements,” IEEE Trans. on Circuits and Systems for Video Technology, Vol. 9, No. 3, pp. 438-450, April 1999.

[13] Y.C. Hu, A. Perrig, and D. B. Johnson, “Ariadne: a secure on demand routing protocol for ad hoc networks,” MobiCom 2002, 2002.

[14] W. Lou and Y. Fang, “A survey of wireless security in mobile Ad-Hoc networks: challenges and available solutions,” book chapter in Ad-Hoc Wireless Networking, Kluwer, 2003.

[15] P. Papadimitratos and Z. Haas, “Secure Routing for Mobile Ad Hoc Networks,” Proc. SCS Comm. Networks and Distributed Systems Modeling and Simulation Conf. (CNDS ’02), 2002.

[16] W. Lou and Y. Fang, “Securing data delivery in ad hoc networks,” International Workshop on Cryptology and Network Security (CANS’03), Miami, FL, 2003.

[17] M.G. Zapata, “Secure Ad Hoc on-Demand Distance Vector Routing,” Mobile Computing and Comm. Rev., Vol. 6, No.3, pp. 106-107, 2002.

[18] P. Papadimitratos and Z. Haas,Securing Mobile Ad Hoc Networks, Handbook of Ad-Hoc Wireless Networks, M.Ilyas, ed., CRC Press, 2002.

[19] W. Wei and A. Zakhor, “Robust Multipath Source Routing Protocol (RMPSR) for Video Communication over Wireless Ad Hoc Networks,” ICME, 2004.

[20] Anit Kumar and Pardeep Mittal, “A Comparative Study of AODV & DSR Routing Protocols in Mobile Ad-Hoc Networks,” International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 5, May 2013, ISSN: 2277 128X.

[21] Dr.A.A.Gurjar andMr.A.A.Dande, “Adhoc on Demand Distance Vector Routing Protocol: A Review Study,” Research Inventy: International Journal of Engineering and Science ISSN: 2278-4721, Vol. 2, Issue 3 (February 2013), Pp 27-29.

[22] Y.C. Hu, A. Perrig, D. B. Johnson,“Ariadne : a secure on demand routing protocol for ad hoc networks,” MobiCom2002, 2002.

[23] K. Sanzgiri, B. Dahill, B.N. Levine, C. Shields, E.M., and Belding-Royer,“A Secure Routing Protocol for Ad-Hoc Networks,” Proc. IEEE Int’l Conf. Network Protocols (ICNP ’02), pp. 78-89, 2002.

[24] Lou, W.; Liu, W., Zhang, Y., & Fan, Y.,“SPREAD: Improving network security by multipath routing in mobile ad hoc networks,” Springer Wireless Networks, Vol. 15, No. 3, 2009, pp. 279-294.

[25] Mavropodi, R.; Kotzanikolaoua, P., &Douligerisa, C., “SecMR- a secure multipath routing protocol for ad hoc networks,” Elsevier Ad Hoc Networks, Vol. 5, Issue 1, January 2007, pp 87-99.

[26] H. Schwarz, D. Marpe, and T. Wiegand, “Overview of the scalable video coding extension of H.264/AVC,” IEEE Trans. Circuits Syst. Video Technol., vol. 17, no. 9, PP. 1103–1120, Sep. 2007.

[27] Jacquet, P., Muhlethaler, P., Clausen, T., Laouiti, A., Qayyum, A., &Viennot, L. (2001). “Optimized link state routing protocol for ad hoc networks,” In Proceedings of IEEE International Multi Topic Conference, 2001. IEEE INMIC 2001. Technology for the 21st Century, (pp. 62–68).

[28] ShapourJoudiBegdillo, Mehdi Asadi, andAbolfazlToroghi, “Improving Packet Delivery Ratio in ODMRP with Route Diversity,” IJCSNS International Journal of Computer Science and Network Security, (Vol.7 No.12) (2007, December).

Open Science Index, Computer and Information Engineering Vol:9, No:6, 2015 publications.waset.org/10002105.pdf