ISSN:1991-8178

Australian Journal of Basic and Applied Sciences

Journal home page: www.ajbasweb.com

Bandwidth Aware Secure Routing Protocol for WMNS

[1]T.M. Navamani and [2]P. Yogesh

[1]*Department of Computer Science and Engineering, Easwari Engineering College, Chennai, Tamilnadu, India*
[2] *Department of Information Science and Technology, Anna University, Chennai, Tamilnadu, India*

ARTICLE INFO

Article history:
Received 12 March 2015
Accepted 28 April 2015
Available online 5 May 2015

Keywords:
Wireless Mesh Networks, Bandwidth, QoS, Trust, Routing Metrics, Attacks

ABSTRACT

This paper describes a Bandwidth aware Secure Routing Protocol for Wireless Mesh Networks (BSRP). Wireless Mesh Networks (WMN) is an emerging technology for next generation wireless networking and it plays a vital role in providing real-time services for the applications running on the networks. Hence, Bandwidth is a significant parameter to satisfy Quality of Service (QoS), and it is considered here for optimal route discovery and efficient packet transmission in WMN. BSRP includes Trust and QoS based routing metrics, secure route discovery, routing table updation and construction. A new metric, named Bandwidth Aware Metric (BAM) is introduced to capture the available bandwidth information, which is the main issue in supporting quality-of-service in WMNs. Security has been a primary concern in order to provide protected communication in wireless mesh networks. A new routing metric called the Mistrust Value (MV) which is computed by Neighbors Passive Acknowledgement Mechanism, is also introduced to address security issues. The simulation results of BSRP show that the discovered route is supporting QoS and also resilient to various packet dropping attacks.

To Cite This Article: T.M. Navamani and P. Yogesh., Bandwidth Aware Secure Routing Protocol for WMNs. ***Aust. J. Basic & Appl. Sci.,*** *9(11): 397-405, 2015*

Introduction

Wireless Mesh Networks (WMN) has recently gained considerable popularity, owing to their ubiquitous networking capabilities. The network is constructed with a wireless mesh backbone and mesh clients. Mesh backbone consists of static mesh routers. Mesh clients are normal wireless or wired clients. The mesh routers have improved computational communication, and power resources, compared to mesh clients. In addition, mesh routers are also typically equipped with multiple radios, and are therefore able to establish high capacity connections (Akyildiz Ian *et al*., 2005). Figure 1 shows the architecture of a wireless mesh network. To access the network and to connect with the internet, mesh clients are connected to one of the end mesh routers available in the mesh backbone. Some of the mesh routers act as gateway nodes to connect with the external networks. To support the next-generation applications with real-time requirements, these networks must provide improved quality of service guarantees. Bandwidth plays a major role in satisfying the QoS and hence finding the path with the maximum available bandwidth is so important to support QoS in WMN. The bandwidth for each link is computed by considering MAC layer measurements (R. Hou *et al*., 2012). The allowable rate of data packet traffic is also depends on the maximum guaranteed bandwidth available in the path. Thus, discovering a path with guaranteed bandwidth is taken as a primary goal in the proposed scheme.

Security is a vital problem in the design of a WMN. The client should have end to end security assurance. However, being different from wired and traditional wireless networks, the WMN could easily be compromised by various types of attacks. Even the WMN infrastructure like the mesh router, could be relatively easily attacked by attackers (Ping Yi *et al*. 2010; Ping Yi *et al*. 2009). Secure routing is the basic and critical aspect of any wireless networks, especially multi hop heterogeneous wireless networks. The range of security threats is more in multi hop networks, compared to the single hop. So, it is very difficult to provide security to such type of networks.

This paper focuses on the problem of identifying bandwidth based secure routing path in WMN. Wireless mesh networks are vulnerable to different types of attacks. The QoS parameter we focus on, in this research work is bandwidth. The goal of the proposed protocol is to find a secure maximum available bandwidth path from the source to the

Corresponding Author: T.M. Navamani, Department of Computer Science and Engineering, Easwari Engineering College, Chennai, Tamilnadu, India

destination to support the necessary quality of service. Two new routing metrics, namely, the Bandwidth Aware Metric (BAM) and Mistrust Value (MV), are introduced to find a secure QoS support path. Broadcasting of routing packets is restricted by considering the Mistrust Value in such a way that control packets overhead is minimized. By considering security, it is possible to avoid a path having more malicious nodes, and thereby prevent packet dropping attacks, such as black hole, grey hole, packet misdirecting attacks and wormhole attacks.

This paper is about finding a bandwidth based secure routing path in WMN. The rest of this paper is structured as follows. Section 2 presents a study of the existing routing metrics and secure routing protocols, while Section 3 introduces the proposed approach. Section 4 details the performance evaluation of the proposed protocol. In Section 5, conclusion of this work is discussed with future research directions.

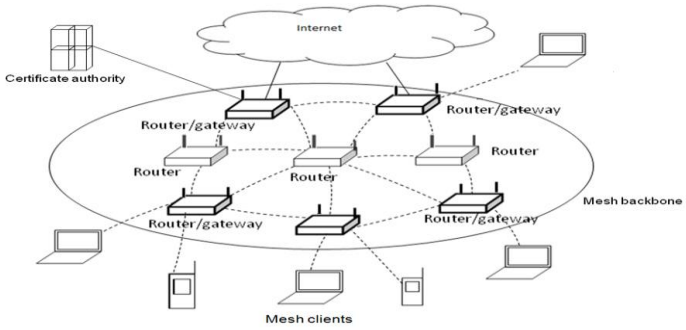

Fig. 1: Wireless Mesh Network Architecture.

Related Work

This section focuses on several existing path metrics which have been developed, for finding out the maximum available bandwidth. This section also discusses the various secure routing protocols available in the literature. R. Darves *et al*. (2004a,b) and D. Couto *et al*. (2008) discussed about several routing metrics designed for WMN with consideration of link quality. Initially, a metric named Expected Transmission Count (ETX) metric is defined, which estimates the number of data transmissions needed to send a packet over the link; Many routing metrics are extended and defined from this metric. Expected Transmission Time (ETT) which is an extension of ETX by considering the packet size and bandwidth and solves the overcomings of ETX. The Weighted Cumulative Expected Transmission Time (WCETT), which is an extension of ETT, was discussed by R. Draves *et al*. (2004a). P. Subramanian *et al*. (2008) proposed a new routing metric, called the Interference Aware Routing Metric (iAWARE), which is an ETT metric adjusted based on the number of interference links. Y. Yang *et al*. (2008) discussed the Interference Resource Usage (IRU) metric, which is an extension of the ETT metric. It is weighted with a number of interference links. It captures the inter-flow interference since it favors a path that consumes less channel times at its neighboring nodes. M. Genetzakis *et al*. (2008) proposed a new routing metric, called the Contention Aware Transmission Time (CATT), which is an extension of Interference Aware Resource Usage (IRU). CATT considers the packet size and data rate on the links. Stefano Paris *et al*. (2013) proposed a novel cross-layer based routing metric, named Expected Forwarding Counter (EFW) to defend against packet dropping attacks. This metric considers link quality of wireless links using Medium Access Control (MAC) layer measurements and also monitors the forwarding behavior in network layer to select high performance secure reliable routing path in WMN. Two further variants of EFW are also proposed in the same paper to solve the problem of packet dropping behaviors of selfish nodes.

The Secure Ad hoc on demand Distance Vector (SAODV) routing protocol is a secure variant of the Ad hoc on demand Distance Vector (AODV) routing protocol, designed by Zapata M.G. *et al*. (2002) for ad hoc networks. SAODV uses the hash chain and digital signature, to secure the mutable field (hop count) and non-mutable field (the rest of the routing message except hop count field), and successfully defends against impersonation attacks, modification of the hop count and sequence number attacks. However, it does not provide hop-by-hop authentication. S.Quazi *et al*. (2008) proposed a new protocol, called the Ticket Based Ad hoc on Demand Distance Vector (TAODV) which secures against both active and passive attacks. It is based on the transfer of the public key between the source and the destination. Ming Yu *et al*. (2009) introduced a new secure routing protocol with quality of service support, called Trustworthiness-based Quality of Service (TQOS) routing, which discovers secured

route using trustworthiness-based QoS routing metrics. Trustworthiness can be established by means of verification done at each node. By using message and route redundancies, most of the internal attacks are detected. However, the procedures for the implementation of the security mechanisms applied in TQOS are not described in detail and the trust values are computed only on the basis of verification done on each node, which will not reveal actual trust value of a node. C. E. Perkins *et al*. (1994) presented an innovative approach the DSDV, which models the mobile computers as routers, which cooperate to forward packets as needed, to each other to build ad hoc networks. T. W. Chen *et al*. (1998) proposed a new routing scheme for wireless ad hoc networks, called Global State Routing (GSR) in which link states are exchanged among their neighbors, during route discovery. S. Khan *et al*. (2010) proposed a Secure Routing Protocol for Wireless Mesh Networks (SRPM), which is based on distance vector routing, and uses an inexpensive two hop passive acknowledgement and two hop information in the routing table of each access point. Here, the compromised nodes attack of the packet header is not considered. Jonathan Loo *et al*. (2009) proposed a Cross Layer Secure and Resource aware On demand Routing (CSROR) protocol, which discovers an optimal route using cross layer based routing metrics, and is also resilient to different packet dropping attacks, but it fails to address packet modification attacks and the scalability problem in wireless mesh networks. Q. Xue *et al*. (2003) proposed a protocol to check the local available bandwidth of each node and to determine whether it can satisfy the bandwidth requirement.

Based on the above review, we conclude that few protocols are capable of defending against internal attacks, by using cryptographic mechanisms, routing metrics and few protocols address QoS issues. The routing protocol which considers both the QoS performance and security for WMN, is still a challenging problem to be solved. In this paper, we propose a new routing protocol that is able to provide QoS by guaranteeing sufficient bandwidth. The proposed protocol also provides security by avoiding the malicious nodes in the path between the source and the destination.

Bandwidth Aware Secure Routing Protocol (BSRP):

A. Network Model:

We consider the WMN architecture at metropolitan-scale and it comprises of three entities: a Trusted Certificate Authority (CA), Mesh Routers (MR), and Mesh Clients (MC). The global topology information of the whole WMN is maintained by the mesh routers by constantly exchanging information with each other. Figure 1 depicts the basic architecture of WMN which includes Certificate Authority, Mesh Routers, Mesh Clients and connectivity with the internet. Initially, each new node has to register with the Certificate Authority by sending its personal details. We assumed that each node initially has a pair of public and private keys issued by Certificate Authority (CA) during its deployment. We further assume that all traffic from source client node to destination client node passes through the routers present in mesh backbone. Initially, each node in the network receives a certificate which is given in the following format from CA.

$$CA \rightarrow N1: \quad Cert_{N1} = [Id(N1), K_{N1+}, t_{Is}, t_{Ex}] K_{CA-}, K_{CA+} \quad (1)$$

The Certificate contains the unique identifier of node N1 assigned by CA, public key of N1 (K_{N1+}), Issue time, Expiration time and public key of CA (K_{CA+}). The Notation [...], in equation (1) denotes that contents specified inside [...] are concatenated and signed by CA. Without having the certificate, the node cannot communicate nor act as an intermediate node. We also consider a scenario that a global passive attacker or an active attacker which can able to eavesdrop all network communications, which can compromise and control a small number of users and mesh routers subject to his choices.

B. Notations:

The notations and their description that are used in the proposed scheme are given in the Table 1.

C. Routing Metrics:

In this section, the proposed routing metrics are described in detail. Our proposed scheme intends to enhance the routing metrics to defend against packet dropping and misdirecting attacks and also to select an optimal path in WMNs. The routing metrics such as Mistrust Value (MV), Bandwidth Aware Metric (BAM) in addition to hop count are implemented during route discovery. Route information in the routing table varies depending on the routing algorithm and the metric used. There may be multiple paths for a single destination; the selection of the best path is done on the basis of the routing metrics. For every one hop neighbors and two hop neighbors, the MV value is computed at each node using Neighbors Passive Acknowledgement Mechanism (NPAM) and updates them in its trust table. If the Mistrust Value (MV) of a node is greater than certain threshold, then it is considered as unreliable. The Route discovery process uses these metrics for selecting an optimal path from source to destination.

Neighbors Passive Acknowledgement Mechanism (NPAM):

Each node in the network maintains a routing table which consists of node's one hop neighbors, two hop and three hop neighbors. Each node computes Mistrust Value (MV) for its one hop and

two hop neighbors by forwarding probe packets to its one hop neighbors, two hop neighbors and getting acknowledgement from its two hop neighbors and three hop neighbors as shown in Figure 2. Source MR1 sends packets to MR2, which in turn forwards to MR3, MR4, but receives passive acknowledgement from MR3 and MR4 to validate the reliability of MR2 and MR3. MV is computed as follows.

Table 1: Notations.

Notation	Meaning
MC	Mesh Client
MR	Mesh Router
CA	Certificate Authority
MV	Mistrust Value
K_{N+}	Public Key of N
K_{N-}	Private key of node N
$Cert_N$	Certificate belonging to Node N
[ ]K_{CA}	Message digitally signed by Certificate Authority CA

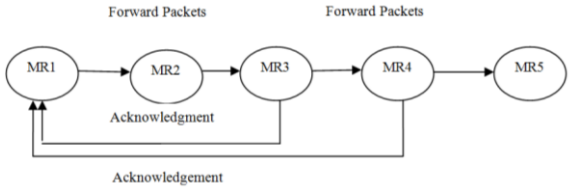

Fig. 2: Neighbors Passive Acknowledgement Mechanism.

Mistrust Value of One hop neighbors MV1= Number of packets forwarded to one hop Neighbors (Npkt1) – Number of Passive Acknowledgements from two hop neighbors(Nack1) (2)

Mistrust Value of Two hop neighbors MV2 = Number of packets forwarded to two hop neighbors (Npkt2) – Number of Passive Acknowledgements from three hop Neighbors(Nack2) (3)

The more MV, the less secure is the node. The Neighbors Passive Acknowledgement Mechanism is resilient to packet dropping and misdirecting attacks like black hole, gray hole and wormhole attacks. In our proposed protocol BSRP, if node MR2 is compromised and acts like a gray hole by selectively forwarding packets (drops some packets), the node MR1 is constantly computing the MV of node MR2. In such a case, node MR1 will not receive some passive acknowledgement (of lost packets) from node MR3 and also from node MR4, which shows that the intermediate node MR2 is compromised and it is acting as grey hole. In case, no passive acknowledgement is received, then node MR2 is black hole.

Bandwidth Aware Metric (BAM):

The computation of BAM metric is described as follows. Let us assume that the bandwidth of the link from Source s to Destination d is B(s, d). Given a path p=<n1, n2, . . . nm>, let WBW(p)=B(p), FBW(p)=B(n1,n2), TBW(p)= WB(< n1, n2, n3 >), and HBW(p) = WB(<n1,n2,n3, n4 >). In other words, WBW (p) is the bandwidth of the whole path, FBW (p) is the bandwidth on the first link, TBW (p) is the bandwidth of the sub path composed of the first two links, and HBW (p) is the bandwidth of the sub path composed of the first three links. Here, the bandwidth metric is computed for every clique found in the network. A clique is a sub path of a routing path in a network. An interference clique is defined as the set of links which interfere with each other. A maximal interference clique is a complete sub graph that is not contained in any other complete sub graph. A routing path in a network consists of two or more maximal interference cliques. (R. Hou *et al*. 2012). The bandwidth of the path is the bandwidth of the bottleneck clique, and here we assume, that a clique consists of three links, and the interference range of each node is a 2 hop count. If there are two routing paths p1 and p2 from s to d, then the condition WBW(p1) ≥WBW(p2) and FBW(p1) ≥ FBW(p2) and TBW(p1)≥TBW(p2) and HBW(p1) ≥ HBW(p2) is called as the pruning condition. This is sufficient condition to determine which path is worthwhile to be advertised. This condition also proves that p2 is not the sub path of any widest path. Hence, p1 is worthwhile to be advertised. The protocol will select the maximum available bandwidth path as the optimal routing path.

Given a path p, the Bandwidth Aware Metric (BAM) of p, denoted by $\vec{w}$(p), is defined as

(w1(p),w2(p),w3(p),w4(p)) where w1(p)=WBW(p), w2(p)=HBW(p), w3(p)=B(p), and w4(p)=FBW(p). $\vec{w}$(p1) ≥ $\vec{w}$(p2) iff w1(p1) ≥ w1(p2), w2(p1) ≥ w2(p2), w3(p1) ≥ w3(p2), and w4(p1) ≥ w4(p2). The maximum available bandwidth path can be found out by finding the non dominated path. That means, if there are two paths p1 and p2, if $\vec{w}$(p1) ≥ $\vec{w}$(p2), then p1 dominates p2. If there is no path dominating p1, then p1 is called as a non-dominated path.

D. Routing Table Construction and Route Discovery Algorithm:

The proposed BAM metric satisfies the isotonicity property, which allows us to develop routing protocol to identify a secure end-to-end path, with the maximum possible bandwidth from each node to each destination. Especially, it finds whether the path is to be advertised, meaning that whether a path is a potential sub path of a widest path. The routing protocol advertises the path information to its neighbors whenever a node finds a new non-dominated path. The routing packet contains the necessary path information. For each non-dominated path p from source s to destination d, s advertises the tuple (s, d, FH (p), SH (p), TH(p), $\vec{w}$(p)) signed by its private key along with its certificate to its neighbors in a route packet, where FH(p), SH(p) and TH(p) are the next hop, the second next hop, third next hop respectively and $\vec{w}$(p) is the computed BAM metric for the clique found. Each neighbor node verifies the signature of the route packet and on successful verification, updates the routing information in the distance table. For the verification process, the neighbor nodes and the destination can get public key of source from its certificate attached with the routing packet. Each node has the information about first four hops by accessing the route packet. Before broadcasting to its neighbors, it checks the trust level of the neighbor nodes in the trust table which is maintained at each node. It broadcasts the routing information only to the neighbor nodes whose trust level is greater than expected threshold level. If the trust level is below the threshold, it does not broadcast the routing information to that node. By means of this process, the control message overhead is reduced. Each node keeps three tables: the distance table, routing table and trust table. Node s puts all the non-dominated paths advertised by its neighbors in its distance table. It keeps all the non-dominated paths found by s itself in its routing table.

By using neighbors passive acknowledgement mechanism, each node computes the trust level of the neighbor nodes by accessing the computed Mistrust Value (MV), which is maintained in the trust table. The trust level for the neighbor nodes are assigned by keeping some constant threshold for the Mistrust value. When s receives a signed advertisement (u, d, FH (p), SH (p), TH (p), $\vec{w}$(p)) from a neighbor node u, which represents a non-dominated path p from u to d, it authenticates the node u by signature verification. If the verification is successful, it removes all the locally recorded paths from u to d which are dominated by p. Denote p' as the path from s to d which is one-hop extended from p. Source s computes the BAM of p' by the formula as discussed in (R. Hou *et al.* 2012). By comparing $\vec{w}$ (p') with the BAM of the paths from s to d in the routing table, s can determine whether p' is a non-dominated path and remove the paths that are dominated by p'. If p' is a non-dominated path, s generates a signed advertisement (s, d, u, FH (p), SH (p), $\vec{w}$ (p')).

The following pseudo code shows the BSRP algorithm, to find out a secure maximum available bandwidth path. Hence each node can find secured QoS aware route by periodically exchanging the routing information. The Trust level metric ensures that the path contains less number of malicious nodes and the BAM metric ensures the maximum available bandwidth path. Thus, the chosen path provides the required quality of service and security.

BSRP Algorithm

```
For each node
    Construct the routing information by computing BAM routing metric.
    Update the routing table
    Compute the trust level of neighbor nodes by using Neighbors Passive
      Acknowledgement Mechanism
    Update the trust table
    Find the neighbor nodes N whose trust level greater than threshold
      Broadcast the signed routing information along with its own certificate to neighbors N
    If trust level of neighbor nodes is greater than threshold then
      Forward Signed Routing information to neighbor nodes
    Else
      Do not forward routing information to neighbor nodes
    End If
    If a node receives advertisement from neighbor nodes then
```

```
    Updates the distance table
  End If
  If the advertised path is non dominated secured path and sequence number is higher
       than the available path in the routing table then
    Advertised path is selected as the routing path and update it in the distance table
  else
    Select the available path in the routing table
  End If
End
```

Performance Evaluation

In this section, we have conducted extensive simulation experiments under NS2 to analyze the performance and security of our proposed protocol BSRP in both normal and malicious network environments and compared it with the TQOS (Trustworthiness-Based QoS Routing Protocol for Wireless Ad Hoc Networks) proposed by Ming Yu *et al*., (2009) and DSDV (Destination Sequenced Distance Vector) routing protocols. TQOS is a Secure Routing Protocol developed for Wireless Ad Hoc Networks in which trustworthiness is incorporated in the routing metrics and QoS parameters are considered during Route discovery. Since our proposed protocol is based on DSDV and we are also proposing QoS Supported Secure Routing Protocol, we have considered these two protocols for comparison. Simulation experiment setup is shown in Table 2.

Table 2: Simulation Parameters.

Parameters	Values
Number of nodes	50
Total Simulation time	200s
Packet size	1000 bytes
MAC Protocol	802.11n
Radio transmission range	250m
Area size	500m×500m
Protocols	BSRP, DSDV,TQOS

To evaluate the performance and security, we have taken the following quantitative metrics in both normal and malicious conditions.

Packet delivery ratio:

The number of packets that are received at the destination to the total number of packets that are sent by the source.

End-to-end delay:

The amount of time taken to transmit a packet from the source to the destination.

Jitter*:*

Variation in the time between packets arriving, caused by network congestion, timing drift, or route change.

A. Performance Analysis:

To analyze the performance, we have taken the scenario of 50 normal nodes with varying traffic loads. The traffic load is varied from 10-60 packets/second, and incremented by 10 packets per second. The results gained from the simulations are illustrated in Figures 4-6.

Packet Delivery Ratio (PDR):

Figure 4 shows the PDR against traffic load, for the BSRP, TQOS and DSDV. At the beginning, when the traffic load was less, e.g., 10 packets per second, all the three protocols display a high packet delivery ratio, and it declines with increasing traffic load. The proposed protocol chooses the path with the QOS support metric such as bandwidth and also by advertising the routing packets to restricted nodes based on trust level, which in turn avoids congestion and increases network resource utilization. Here, BSRP and TQOS shows similar performance compared to DSDV, when the traffic load is higher. Since TQOS provides security and also QoS support during packet transmission, it also gives better performance. With varying traffic load, BSRP maintains the PDR above 85%. This shows that the BSRP gives a better performance in delivering packets though the nodes having high mobility.

End-to End Delay:

Figure 5 demonstrates the average end-to-end delay of packets, to travel from the source to the destination's application layer. It can be observed that the end to end delay of BSRP is better than that of TQOS and DSDV. At a low traffic load, the three protocols perform identically. However, with increasing traffic load, the performance of BSRP becomes better than that of TQOS and DSDV, since the packets are transmitted over a stable path in the proposed protocol. By restricting the broadcasting of control packets based on

Mistrust Value during route discovery, the routing overhead is minimized and hence end-to-end delay is minimized in BSRP. In TQOS, security, QoS mechanisms and Trustworthiness metrics are implemented during route discovery, the computation overhead is maximum which in turn gives large end-to-end delay. DSDV is a basic routing protocol without providing security, where the end-to-end delay is high since the protocol is more vulnerable to active attacks.

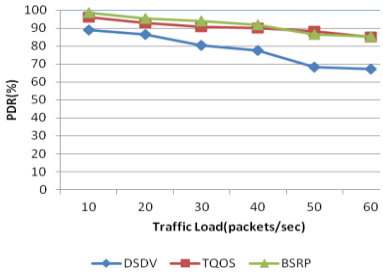

Fig. 4: Packet Delivery Ratio Vs Traffic Load.

Fig. 5: Average End-to end delay Vs Traffic Load.

Delay Jitter:

Figure 6 shows the delay jitters for BSRP, TQOS and DSDV. The smallest jitter is observed in the case of BSRP, since the packets are transmitted over the QoS aware path, and also congestion is avoided by minimizing the control message overhead. TQOS also shows better performance compared to DSDV since the route discovered by TQOS is more secure and QoS supported path. The DSDV has a higher delay jitter than the other two protocols, because of its higher congestion. Since the path found by DSDV is more prone to active and passive attacks, the latency is more which in turn leads to worse congestion.

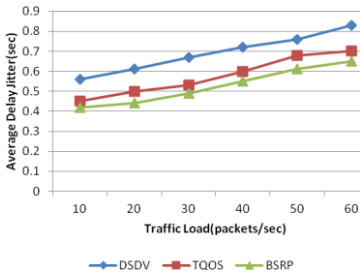

Fig. 6: Delay Jitter Vs Traffic Load.

B. Security Analysis:

To analyze the security of the proposed protocol against the attacker nodes, we have taken various network scenarios, by varying the malicious nodes from 5 to 20 out of 50 nodes. The above discussed parameters are again considered for the security analysis.

Packet Delivery Ratio:

The Packet Delivery Ratios (PDR) for the BSRP, TQOS and DSDV are shown in Figure 7. It can be seen that BSRP and TQOS consistently outperforms DSDV. The packet delivery ratio of BSRP and TQOS is nearly 98% when the number of malicious node is 0. When the numbers of malicious nodes are increased, the PDR drops at various levels for all the three protocols. But the BSRP and TQOS almost maintain a constant performance for the PDR, when the nodes are increased from 10. The proportional increase in the malicious nodes decreases the PDR % linearly as shown in Fig. 9.

Since the BSRP finds the secure and maximum available bandwidth path, the performance is maintained with good results, even in the presence of malicious nodes.

End-to-end Delay:

The end-to-end delay of BSRP, TQOS and DSDV is measured in terms of mille seconds (ms) as shown in Figure 8. To compute the end-to-end delay, different scenarios are generated using the setdest tool. A longer end-to-end delay is observed in the case of DSDV. When the numbers of malicious nodes are increased, the DSDV experiences more delay due to the lack of QoS support and security. The BSRP shows an improvement compared to the TQOS and DSDV, since the path is protected from malicious nodes, maximum available bandwidth and also minimizing the control message overhead.

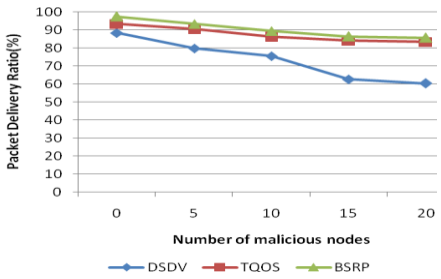

Fig. 7: PDR Vs No. of malicious nodes.

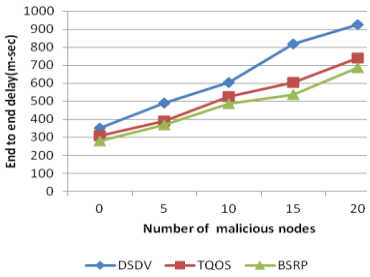

Fig. 8: End to end delay Vs No. of malicious nodes.

Conclusion

In this paper, we have proposed two new routing metrics, viz, Bandwidth Aware Metric (BAM) which supports QoS and Mistrust Value (MV) which addresses the security issues. The routing protocol based on BAM and MV discovers the secure maximum available bandwidth routing path. By implementing Neighbors Passive Acknowledgement Mechanism (NPAM), most of the packets dropping attacks are prevented. The proposed protocol satisfies the optimality and consistency requirements. A comparison of the BSRP with two different routing protocols, viz, TQOS and DSDV is done using ns-2. The comparison covers most of the parameters such as the Packet Delivery Ratio, Average End-to-end delay, and Delay jitter, with and without malicious nodes. The performance of the protocols is analyzed according to varying traffic loads in a non- malicious environment and varying malicious nodes in malicious environment. The BSRP and TQOS provide similar better performance with all the taken parameters except end-to-end delay. The proposed protocol minimizes the end-to-end delay by minimizing the control message overhead. Both these protocols outperform DSDV because of Security mechanisms and QoS support. The proposed protocol provides better security against various packet dropping attacks, such as gray hole, black hole and wormhole attacks. Thereby the proposed protocol BSRP selects a secure maximum available bandwidth path, to satisfy efficient quality of service. By adding some cross layer metrics and other QoS support parameters, the proposed protocol can be further enhanced.

REFERENCES

Akyildiz Ian, F., Xudong Wang, Weilin Wang, 2005. Wireless Mesh Networks: A Survey, Elseveir Science, Computer Networks, 47: 445-487.

Hou, R., King-Shan Lui, F. Baker, Jiandong Li, 2012. Hop-by-hop routing in wireless mesh networks with bandwidth Guarantees. IEEE Transactions on Mobile Computing, 1(2).

Ping Yi, Yue Wu, Futai Zou, Ning Liu, 2010. A Survey on Security in Wireless Mesh Networks, IETE Technical Review, 27.

Ping Yi, S., Tianhao Tong, T. Ning Liu and H. Yue Wu, 2009. Security in Wireless Mesh Networks: Challenges and Solutions. IEEE 6th International

Conference on Information Technology: New Generations, ITNG'09.

Hansman, S., R. Hunt, 2005. A Taxonomy of Network and Computer Attacks Computers and Security. Elsevier, 24(1): 20-31-43.

Draves, R., J. Pandhye, B. Zill, 2004a. Comparison of routing metrics for static multi hop wireless networks, ACM SIGCOMM September, 133-144.

Couto, D., D. Aguayo, J. Bicket, R. Morris, 2008. A high throughput path metric for multi-hop wireless mesh networks. ACM MOBICOMM, 134-146.

Draves, R., J. Padhye, B. Zill, 2004b. Routing in multi-radio, multi hop wireless mesh networks. ACM MOBICOMM, 114-128.

Subramanian, P., M.M. Buddhikot, S. Miller, 2006. Interference aware routing in multi-radio wireless mesh networks. IEEE W iMesh, 55-63.

Yang, Y., J. Wang, R. Kravets, 2008. Designing routing metrics for mesh networks, IEEE INFOCOM, 2288-2296.

Genetzakis, M., V.A. Siris, 2008. A contention-aware routing metric for multi-rate multi-radio mesh networks, IEEE SECON, 242–250.

Stefano Paris, Cristina Nita-Rotaru, Fabio Martignon and Antonio Capone W. Luo, 2013. Cross-Layer Metrics for Reliable Routing in Wireless Mesh Networks. IEEE/ACM Transactions on Networking, 21-3.

Zapata, M.G., N. Asokan, 2002. Securing ad hoc routing protocols, Proceedings of 1st ACM Workshop on Wireless Security (WiSE'02).

Quazi, S., Yi Mu, W. Susilo, 2008. Securing wireless mesh networks with ticket based authentication. International Conference on Signal processing and Communication Systems, 1-10.

Ming Yu, Kin K. Leung, 2009. A Trustworthiness-Based QoS Routing Protocol for Wireless Ad Hoc Networks, IEEE Transactions on Wireless Communications, 8(4).

Perkins, C.E., P. Bhagwat, 1994. Highly dynamic destination sequenced distance vector routing (DSDV) for mobile computers, Proceedings of the ACM SIGCOMM.

Chen, T.W., M. Gerla, 1998. Global state routing: a new routing scheme for ad hoc wireless networks, IEEE International Conference on Communications (ICC), 171-175.

Khan, S., Kok-Keong Loo, N.M. Naeem, 2010. SRPM: Secure Routing Protocol for IEEE 802.11Infrastructure based wireless mesh networks. Springer Science, 190- 209.

Jonathan Loo, Shafiullah Khan, 2010. Cross layer secure and resource-aware on-demand routing protocol for hybrid wireless mesh networks, Springer Science, 201-214.

Xue, Q. and A. Ganz, 2003. Ad hoc QoS on-demand routing (AQOR) in mobile ad hoc networks, Journal of Parallel and Distributed Computing, 154-165.