Trust Based HWMP Protocol in High-Performance Wireless Mesh Networks

Parimalla Subhash[1] and S. Ramachandram[2]
(Corresponding author: Parimalla Subhash)
Department of CSE, Jyothishmathi Institute of Technological Sciences[1]
Karimnagar, India
(Email: subhash.parimalla@gmail.com)
Department of CSE, UCE, Osmania University[2]
Hyderabad, India
(Received Sept. 6, 2015; revised and accepted Nov. 12, 2015)

Abstract

Wireless mesh networks are multi hop wireless networks with high performance requirements. To enhance the performance, a large number of routing protocols have been proposed focussing on various link properties.The metrics designed to capture various link properties make an important assumption that nodes cooperate in network operations. On the other hand, the nodes are spread over larger area and maintained by different operators which lack cooperation leading to selfish and malicious behavior. To address this issue, several works have been carried out by modelling trust/reputation into a network. In this paper, we modify an existing trust based secure routing framework, AODV-REX, tailored to mesh networks, as a first step. We observe that the existing trust models for distributed wireless networks are not directly employable and need to be significantly modified to meet the performance requirements of mesh networks. Further, we propose a trust extension to HWMP (Hybrid Wireless Mesh Protocol), called HWMP-TX based on a new trust model. The analysis and simulation results show that HWMP-TX is resilient to various internal attacks and achieves better performance.

Keywords: HWMP, reputation, secure routing, trust, wireless mesh network

1 Introduction

Wireless Mesh Network (WMN) is a multi-hop wireless network that inherits self-healing, and self configuring capabilities from mobile ad hoc network (MANET). Besides these, the additional features of WMN include static, and non-power-constrained nature of mesh routers. WMN also lowers the deployment cost and administrative overhead by replacing the majority of the wired infrastructure. These features make them an ideal candidate solution for providing wireless broadband internet access in an office, campus or community networks, without requiring every access point to be physically connected to the Internet [2]. Thus, WMN technology has generated a huge amount of interest in the industry and academic fields due to its suitability to various commercial application scenarios.

On the other hand, there are many other issues that need to be addressed to make WMNs commercially successful. Design of an optimal routing protocol is one such issue that requires immediate attention. As WMNs are expected to support high performance internet applications, routing protocol and the employed routing metric plays a dominant role in determining the amount of throughput achieved. Several routing protocols have been proposed in conjunction with different routing metrics to increase the overall performance of the network [5, 6, 11, 25].

Design of routing metrics for WMN mainly involves accounting for the physical properties of a wireless link that usually affect the network performance. It should also account for the features that indirectly contribute to the network performance. Properties, mainly, link variability, varying available bandwidth and flow interference (inter and intra) should be considered to maximize throughput [22]. The design of routing metric that results in optimal performance assume that all nodes are honest and well behaved in the route selection process. This is not a valid assumption in a distributed network like WMN, where nodes operate in an open wireless environment. Nodes tend to exhibit selfish and malicious behavior, and needs to be accounted to enhance performance.

Routing misbehavior is one major issue in any distributed network like WMN. The existence of selfish nodes is justified due to the presence of nodes from multiple operators in a commercial WMN. These nodes may intentionally drop the packets, forwarding their own traffic. Nodes can also be easily compromised by an adversary,

due to the open environment in which they operate. To overcome these kinds of routing mis-behavior, variety of protocols have been proposed particularly by employing trust or reputation in routing activity [1, 8, 12, 14, 17, 18, 24]. The way these protocols employ trust in the routing process depends on the network requirements. For example, in a MANET, where the focus is on maintaining end-to-end connectivity, protocols directly employ trust to select relatively higher trustworthy paths. In a WMN, trust modeling is more complicated because of their need to support high performance applications.

Routes established in a WMN should meet the throughput requirements as well as the trust criterion of the network. In such a scenario, employing trust as the sole metric in route selection process may meet trust requirements, but fail to achieve desired throughput, as the employed metric ignores wireless link characteristics. Integrating trust value of a node/link with the underlying routing metric is an alternate way of discovering routes [17, 18]. But, this integration scheme also does not achieve good results and these two entities (routing metric and trust) are independent and if integrated fail to achieve optimal performance in certain cases.

In this paper, we observe that the existing trust models for distributed wireless networks are not directly employable and need to be significantly modified to meet the performance requirements of mesh networks. As a first step, we modify an existing trust based routing framework, AODV-REX, tailored towards mesh network. Further we propose a trust extension to HWMP, called HWMP-TX based on a new trust model. It complements the link-quality-based routing metric in making routing decisions and achieves better performance over existing approaches to employ trust. We specifically focus on HWMP along with airtime link metric, as it is the mandatory routing protocol to be implemented, according to IEEE 802.11s draft standard for 802.11 based mesh networks [15]. The analysis and simulation results show that HWMP-TX is resilient to various internal attacks and achieves better performance. The performance of both the models is evaluated under various attack scenarios.

The rest of the paper is organized as follows. Related work is discussed in Section 2. Internal attacks against HWMP are presented in Section 3. In Section 4, we propose our modifications to AODV-REX framework that integrates the reputation metric with high throughput path selection metric like airtime. Later, in Section 5, we propose a complete trust model based on an alternate mechanism to employ trust. Performance evaluation and security analysis is presented in Section 6. Experimental results in comparison with existing model are discussed in Section 7. Discussion of several factors is included in Section 8. Finally, Section 9 concludes the paper.

2 Related Work

Lately, a lot of research has been carried out to increase the performance of routing protocols for WMN.The main design goal of these protocols is throughput maximization. Numerous link-quality-based routing metrics have been proposed replacing hop count, to increase the overall throughput, as it has been shown that the hop count selects sub-optimal routes [5]. Metrics such as ATLM (airtime link metric) [16], ETX (expected transmission count) [5], ETT (expected transmission time) [6], WCETT (weighted cumulative ETT) [6] and mETX (modified ETX) [25] have been developed replacing hop count. The main design aim is to enhance performance and increase throughput. The existing reactive and proactive routing frameworks are modified accordingly to accommodate the designed metrics. For example, multi-radio link quality state routing protocol (MR-LQSR) is based on optimal link state routing protocol (OLSR), enhanced to accommodate multiple radios and WCETT routing metric. These metrics are modelled by assuming the co-operation among participating nodes. This is an optimistic assumption in a distributed network like WMN where nodes operate in an open environment, and the possibility of nodes being compromised by an adversary cannot be ignored.

The problem of routing security and node misbehavior has been studied by different researchers, e.g., [1, 8, 12, 14, 17, 18, 24]. Various trust based routing protocols have been proposed for ad hoc and WMNs to mitigate the influence of these malicious nodes in the route selection process.

The distributed trust model proposed by Rehman et al. [1] assumes discrete levels of trust. It employs a decentralized approach to manage trust and a recommendation protocol to exchange trust related information. The model is based on a conditional transitive trust relation that uses trust categories to express trust towards other agents. In order to establish trust relation between entities where a direct relation does not exist, the agents can make use of an intermediate agent to establish trust. Various trust models that exist in the literature try to quantify the trust relationships according to different applications security requirements.For example, the PGP style authentication schemes with certification chains use binary trust valuation

Zheng et al. [24] proposed a trust model that assigns quantitative trust value to each node based on the observed behavior. A node evaluates its relationship with other nodes in a network, based on factors such as experience statistics (es), data value (d), intrusion detection result called intrusion black list (ibl) and references (r) along with a node's preference and policy. Each node maintains a trust matrix to store the knowledge accumulated on the above factors for every other node in the network with the help of network traffic monitoring and recommendations. That is, every node maintains trust relations with all other nodes in the network. Final trust

evaluation of node i to node j for an action a is evaluated through a linear equation that uses the values stored in the trust matrix. The evaluated trust values are used for making better routing decisions. As, each node maintains a list of values for various factors for every other node in the network, the overhead in decision making is very high.

TAODV proposed in [8] is a trusted extension to AODV. The path selection process is similar to AODV with trust replacing hop count as the routing metric. The trust values of nodes are assumed to be distributed in prior. Hence, it does not model the way trust relations are established and fostered. To incorporate trust into the route selection process, the route request ($RREQ$) header is modified to include a trust level field in the AODV RREQ. When a node receives a RREQ, it rebroadcasts it after modifying the trust level field with the trust value of the node from which it received the RREQ. Every node checks back the rebroadcasted RREQ from its previous node to see whether it has provided the proper information. If not, it sends a route warning message questioning the sanctity of the node. The final route selection is based on trust level metric. The major drawback of this model is the prior distribution of the trust levels. Moreover, there is no mechanism to modify the established trust-levels depending on the change in nodes' behavior.

Eissa et al. [7] proposed FrAODV,a friendship based AODV protocol to establish secure paths. It is similar to that when a person (X) wants to verify another person (Y),he generally asks his friends about this person. He also asks this person to provide him with the list of reference persons,who will be asked if he is to be trusted. This protocol uses two algorithms i.e FwEvaluate algorithm to evaluate the forward routes and the RvEvaluate algorithm to evaluate reverse routes in AODV protocol.

Meka et al. [14] proposed a trust framework for AODV that employs trust as the routing metric instead of hop count. According to this framework, a node maintains trust relationships with its neighbors. It also allows a node to assign trust levels to the routes that it discovers. Each node maintains a neighbor trust table (NTT) to store the neighbor ID, its trust value and the current number of RREQ's it can send. In addition to maintaining the NTT, the routing table is modified to include all the routes from that node to a destination, to incorporate route trust. Each node keeps track of the number of packets it has forwarded through a particular route. Trust relations are evaluated with the help of a route acknowledgement RACK that a destination node periodically sends addressed to the source, which contains the number of packets received till that time instant. All the intermediate nodes along the reverse route make use of the RACK to compute the route trust. Whenever a node generates or forwards a RREP, it advertises its trust value (ATV) on the route under consideration to its immediate upstream node. Based on the ATV and the observed trust value (OTV), a node updates the node trust for that neighbor.

Two-Hop acknowledged routing protocol (2-HARP) proposed in [26] is based on zone routing protocol.In 2-HARP, each node maintains trust relations with all the nodes in its 2-hop neighborhood using the neighbor sensing mechanism of OLSR [4]. Each node maintains an acknowledgement table in addition to the routing table. The acknowledgement table is used to store information about packets waiting to be acknowledged. A node after sending a packet, expects a signed acknowledgement from the 2-hop neighbor on the established route, to verify whether the one hop neighbor on the established route, has indeed forwarded the packet. If the one hop neighbor intentionally drops a 2-hop acknowledgement, the 2-hop neighbor tries for a maximum of s times before labelling the node as non-responsive. The main drawback of this model is the acknowledgement overhead. As, each data and control packet is acknowledged twice, it incurs very high overhead.

Tan et al. [23] proposed a trust reasoning model based on fuzzy Petri net is presented for the evaluation of trust values of mobile nodes. In addition, to avoid compromised or malicious nodes, a trust based routing mechanism is proposed to select a path with the highest path trust value among all available paths. Further, OLSR is extended by using the proposed trust model and trust based routing mechanism, called FPNT-OLSR. For the implementation of FPNT-OLSR, a trust factor collecting method and trust information propagating method is designed, which do not generate extra control messages.

AODV-REX proposed in [17] is a reputation based extension to AODV for WMNs. Acoording to AODV-REX, a node maintains two different kinds of reputation values for each of its neighbors (local and global).Local reputation of a neighbor is based on nodes' direct observations using a watchdog [12]. Global reputation of a node is computed based on reputation values obtained from other nodes in the network. Whenever a node requests for a route towards a destination, it transmits a RREQ by appending the reputation values and addresses of all its neighbors. An intermediate node that receives a broadcasted RREQ, acts on the reputation values of interest in the RREQ and ignores the rest leaving them unmodified. It re-broadcasts the RREQ by further appending it with the reputation values of its neighbors. The hop-count metric is modified to accommodate the reputation of a node. The basic idea is to create a new virtual distance that takes into account the reputation level of the node connected to the link. The distance between two neighboring nodes increases if the reputation of one of the node decreases and so the route will be less considered. AODV-REX incurs huge routing overhead as each intermediate node appends the RREQ with the trust values of all its neighbors, thus increasing its size enormously. It is also based on hop count metric that has been shown to select sub-optimal routes

EFW (expected forwarding counter) proposed in [18] is a cross-layer metric for routing in WMN that considers malicious and selfish participants. It employs watchdog to monitor the forwarding behavior of its neighbors. The

forwarding ratio of a node is integrated with ETX (estimated transmission count of a link) to derive a cross-layer routing metric called as EFW. To summarize, for calculating EFW of a link a node needs to monitor its neighbors, calculate its forwarding ratio, and integrate that value with the existing ETX metric.

A key point to note is that in all of the above existing work, trust is either directly employed or integrated with the employed routing metric. Even the attempts to integrate trust with the routing metric have been made on hop count except EFW, where the forwarding probability of a node is integrated with high throughput metric, ETX. In Section 5 , we present an alternate mechanism to employ trust in the routing process that is shown to perform better on average than the attempts to integrate with the routing metric.

Moreover, the majority of the frameworks discussed above employ watchdog to evaluate trust relations, which restricts the nodes from efficiently using the available resources thus affecting network performance.

3 Internal Attacks on HWMP

In this section, we focus on various possible attacks on HWMP (Hybrid Wireless Mesh Protocol). We specifically focus on HWMP as it is the mandatory routing protocol for IEEE 802.11s based mesh networks. We specially concentrate internal attacks, as the authentication protocol at the MAC layer acts as a first layer of defense against attacks from external nodes. Before discussing the various internal attacks, a brief overview of HWMP is provided to understand the operation of the protocol.

3.1 Overview of HWMP

HWMP is a hybrid wireless mesh protocol [3] that operates at layer-2 and employs MAC addresses for path selection. It is called a hybrid protocol as it combines both reactive and pro-active routing strategies. It combines the flexibility of on-demand route selection with proactive topology tree extensions. The combination of reactive and proactive elements of HWMP enables efficient path selection for a wide variety of mesh networks. HWMP is based on ad hoc on-demand distance vector (AODV) protocol adapted for MAC-address based path-selection and link metric awareness [19].

HWMP provides two modes of operation, they are on-demand mode and proactive mode. These two modes are not exclusive and are used concurrently, because the proactive modes are extensions of the on-demand mode. HWMP uses four different kinds of information elements (IEs). Path Request (PREQ), Path Reply (PREP) and Root Announcement (RANN) are employed in path-selection process, while Path Error (PERR) is used for route-maintenance. In HWMP, a path to the destination is described by the next hop at every intermediate mesh station (mesh STA). When a source wants to send data to a destination for which it does not have a path yet, it initiates a path discovery by broadcasting a PREQ.The PREQ Information Element is shown in Figure 1 contains various fields out of which Hop Count, Element TTL, Metric and the Target-Only sub field in Per Target field are operated upon by intermediate nodes as part of the path selection process.

The hop-count field is acted upon by every intermediate node along the selected path. Its value is set to an integer equal to the number of hops from the originator STA to the mesh STA transmitting the PREQ.Element TTL field indicates the remaining number of hops allowed for the PREQ element. It is mainly used to prevent the PREQ element from traversing the network endlessly. Initially, the value of TTL element is set to a number equal to the network diameter. The metric field is set to the cumulative metric from the originator to the mesh STA transmitting the PREQ. The IEEE 802.11s specifies the use of air-time link metric (ATLM) as the default link metric to identify an efficient radio-aware path. All the above discussed fields are modified by the intermediate nodes accordingly, enabling better path selection.

3.2 Attacks on HWMP

HWMP is prone to a number of security attacks from internal malicious nodes. A compromised node becomes an epicentre for launching a variety of attacks, thus degrading the network performance rapidly. Attacks are usually aimed at disrupting the normal network operations. The various kinds of internal attacks are discussed below.

3.2.1 Flooding

It is one of the most simplest and efficient attack. In HWMP, a node can generate any number of PREQs. Malicious nodes can exploit this and flood the network with a number of PREQ's for non existing nodes. A legitimate node would be forced to spend majority of its time processing the PREQ's, resulting in severe performance degradation [20]. Such an attack can be countered by limiting the number of PREQ's that a node can generate based on its trust level.

3.2.2 Modification Attacks

Malicious nodes can redirect network traffic, and launch DoS attacks by altering the fields in IEs. For example, a malicious node can modify the metric field in the PREQ element to include itself in the selected path. Once included, it can launch various other packet dropping attacks. Such attacks can be specifically called as metric manipulation attacks. As, nodes need to cooperate in determining the metric of a path, malicious nodes can exploit this to their advantage. The sequence number of a PREQ message can be modified by a malicious node to a value much higher than that of the destination's current sequence number, thereby fooling the originator of

Element ID	Length	Flags	Hop Count	Element TTL	PREQ ID	Org.Mesh STA.Addr.	Org. HWMP Seq.NO
Org.Ext Addr	Life Time	Metric	Target Count	per Target addr #1	Target Address #1	Target HWMP Seq.No	.....

Figure 1: PREQ element

the PREQ to believe that the manipulated PREP as genuine. There is no way to distinguish between path replies generated by an intermediate node and the destination node, therefore this attack has significant impact on the selection of network paths.

3.2.3 Wormhole Attacks

Wormhole is a hypothetical channel formed between two colluding nodes. The main aim of this attack is to disrupt the routing functionality of a network. A Wormhole can be created by simply tunnelling messages between two colluding nodes, or by transmitting them on an out-of-band channel or by just relaying packets [10, 13, 21]. Once a wormhole is established, the two colluded nodes at the either ends of the tunnel can use this channel to influence path selection decisions. A malicious node can tunnel a PREQ through an out-of-band channel and replay it at the other end. As a path formed through these colluded nodes inherently offers better metric over other available paths. Once, a path is established, the colluded nodes can launch various packet dropping attacks.

3.2.4 Fabrication Attacks

A malicious node can fabricate messages to disrupt the network operations. For instance, a malicious node can fabricate a PERR message that is actually used to notify the nodes along the downstream that the next hop to the originator of PERR is currently unavailable. Nodes receiving such a message will mark the link as broken and re-initiate path discovery. As, cryptographic solutions cannot prevent such kind of internal malicious attacks, an efficient detection mechanism is required to detect and exclude the malicious node. Employing trust to detect such malicious behavior has attracted much research attention and several trust frameworks have been developed to address this issue. Even though several trust frameworks exist in literature, they cannot be directly employed due to the high performance requirements of WMN. Therefore, there is a need for a framework that concurrently focuses on performance requirements on the one hand and trust requirements on the other.

4 Modified AODV-REX for Wiress Mesh Networks

HWMP, the routing protocol for WMN is based on AODV and AODV-REX is a reputation based extension to AODV that integrates reputation of a node with the hop count. As, hop count has been shown to select sub-optimal paths, we attempt to modify AODV-REX for WMN by integrating reputation of a node with airtime metric (ATLM) [3]. We refer to this modified AODV-REX as HWMP-REX. The airtime link metric is a measure for the amount of the consumed channel resources when transmitting a frame over a particular wireless link. The following Equation (1) is used to calculate airtime metric of each link.

$$C_a = \left[O_{ca} + O_p + \frac{B_t}{r}\right] \frac{1}{1 - e_{pt}}. \quad (1)$$

The airtime cost for each pair wise link C_a is calculated in terms of the modulation rate (r) and bit error rate e_{pt} for a test frame of B_t size. Where, O_{ca} is the channel access overhead, O_p is the protocol overhead. O_{ca}, O_p and B_t are constants defined for each 802.11 modulation type.

4.1 HWMP-REX

The proposed modifications are primarily concerned with integrating reputation of a node with airtime rather than hop count. The reputation model and the reputation dissemination process of AODV-REX are left unmodified. AODV-REX employs a multi-layered model for estimating the reputation of network nodes, called REFACING (RElationship-FAmiliarity-Confidence-INteGrity) [16]. It maintains two kinds of reputation values for its neighbors-local and global. Local reputation of a neighbor is based on node's direct observations using a watchdog [12]. Global reputation of a neighbor is computed from reputation values provided by other nodes in the network.

As described in Table 1, when a node has data to send, it generates a PREQ message. Together with the usual HWMP information, a node appends the reputation and addresses of its neighbors to the PREQ message. Upon reception of such PREQ, a node acts on the reputation values of interest and ignores the rest leaving them unmodified. In addition to the reputation values, a node

also acts on the metric field of the PREQ message, as part of the normal process of processing a PREQ. The metric computation process is modified to include the reputation of a node from which it received the PREQ. The modified reputation metric (RM) of a link from node A to node B is given by Equation (2).

$$RM\left(\overrightarrow{AB}\right) = [(1 - R_{B_A}) * AD] \quad (2)$$

R_{B_A} is the reputation of a node B in A and AD denotes the Airtime Diameter. Airtime Diameter is the airtime taken for a standard frame to traverse between two ends of the network. AD can be computed with the help of a test frame, transmitted by setting the TTL equal to the network diameter, at the time of network initialization. The reputation metric of a link is added to the airtime of a link to get the resultant metric. As, the reputation of a node decreases, the reputation metric of a link increases, increasing the overall airtime thus avoiding malicious nodes.

4.2 Issues in HWMP-REX

In HWMP-REX, one of the major issue is computing airtime diameter, AD, of a network. Determining AD is a complex task as it has to be calculated after the network has been initialized. Whenever new nodes are added, the airtime diameter needs to be re-computed for determining overall routing metric of a path. The other important issue is high fluctuations in path selection. This behavior is due to the fact that, HWMP-REX selects a path $\overrightarrow{P_o}$ based on the cumulative metric obtained by integrating reputation of a node with airtime metric of a link. This can be represented using Equation (3), where $l_{s-j(airtime)}$ gives the airtime of a link l_{s-j} and $RV_{l_{s-j}}$ gives the reputation of a node S in J associated with the link.

$$\begin{aligned} RM\left(\overrightarrow{P_o}\right) &= \sum_{L_{\overrightarrow{P_o}}} \left(l_{s-j(airtime)} \oplus RV_{l_{s-j}}\right) \\ &= \left(l_{s-j(airtime)} \oplus RV_{l_{s-j}}\right) \\ &\quad + \left(l_{j-k(airtime)} \oplus RV_{l_{j-k}}\right) + ... \\ &\quad + \left(l_{n-d(airtime)} \oplus RV_{l_{n-d}}\right) \end{aligned} \quad (3)$$

As, both components of Equation (3) play an equal role in path selection process, falsely penalizing genuine nodes result in path fluctuations. As, no lower bounds are established for HWMP-REX to distinguish malicious behavior from normal behavior, it naturally prefers nodes with high reputation over nodes with lesser reputation. In such cases, HWMP-REX prefers a path with better overall cumulative metric over a path that actually achieves higher throughput, which indirectly is a false positive. Existence of lower bounds allows the system to differentiate malicious behavior from normal, which in turn allows the network to chose a lesser reputation node due to its higher link quality. These bounds cannot be established for HWMP-REX, as the path selection decision is based on integrated metric that strictly prefers high reputation nodes over nodes with relatively lesser reputation. To overcome these limitations, we propose a new trust based routing approach that is based on an alternate mechanism to employ trust in routing process.

5 The Proposed Secure Routing for WMN

The proposed secure routing scheme for WMN is based on a new trust model that employs a different approach to employ trust in the route selection process and defends internal attacks.

5.1 Proposed Trust Model

The proposed trust model complements HWMP with its trust observations and allows it to select high throughput trustworthy paths without integrating with the airtime link metric. The trust model comprises of three different phases that are carried out independently without intervening with the routing process. Those are Initialization, Trust Evaluation and Trust Recommendation. The various symbols used in this paper are given in Table 2.

Table 2: Symbols used and their meaning

Symbol	Meaning
U_{ij}	Initial Trust Value
V_{ij}	Current Trust Value
β_{ji}	Packets received by i from j during time interval $TE_{interval}$
$TE_{Interval}$	Trust Evaluation Interval
ε_l	Expected Loss in the Network
δ	Small Fractional Value
Υ_l	Lower Threshold Value
Υ_u	Upper Threshold Value
τ_l	Tolerance Level
ψ_{ij}	Revised Trust Value of j in i

5.1.1 Initialization

A node I after discovering its set of neighbors $\{J\}$, initializes them to a trust value (U_{ij}) of 0.5. The value 0.5 is justified as a node neither trusts nor distrusts the neighbor. The maximum trust value that a node can attain is 1.

5.1.2 Trust Evaluation

Each node periodically evaluates the behavior of its neighbors using the trust evaluation procedure given in Algorithm 1. The evaluation procedure is carried out independently by each node and the evaluation timing of nodes

Table 1: HWMP-REX path selection process

Executed at the source node S initiating Path Discovery process
1: Create a PREQ element by appending the reputation and addresses of all the neighbors of S. **2:** Set the Metric field to 0. **3:** Broadcast the PREQ.
Executed at the intermediate node J upon receipt of the PREQ
1: Parse the PREQ element to act on the reputation fields with which J shares neighborhood. **2:** Update the global reputation of those nodes. **3:** Append the PREQ element with the reputation values and addresses of Js neighbors. **4:** Update current link metric: Metric = currentMetric + (RM + airtime) **5:** ***if***(*Route to source is available*) *then* Unicast PREP Rebroadcast PREQ **6:** ***else*** Rebroadcast PREQ
Executed at the Destination node D upon receipt of PREQ
1: Parse the PREQ element to act on the reputation fields with which D shares neighborhood. **2:** Update the global reputation of those nodes. **3:** Include current link metric: Metric = currentMetric+(RM+airtime) **4:** Choose a path with the best metric. **5:** Unicast the PREP.

need not be synchronized. The evaluation of a neighboring node's behavior is based on the assumption that all the nodes in the network are fairly loaded. This assumption is justified in a WMN as wireless mesh routers are dedicated routers that provide continuous access services to its clients when they are in operational mode. Hence, the contribution of every genuine node in forwarding the network traffic is approximately equal. According to the trust model, a node monitors the performance of its neighbors during an interval of time denoted by $TE_{interval}$. During this time interval $TE_{interval}$, an evaluator node I expects a fixed number of packets α_{ji} from each of its neighboring nodes J periodically. A node also considers the transient losses in the network due to congestion, collisions and errors in the network channel denoted by ε_l .

At the end of the time interval $TE_{interval}$, node I computes the difference between number of packets actually received (β_{ji}) from neighbor J to the packets estimated. After accommodating network losses, if β_{ji} does not confer with estimate α_{ji} , then the additional drop in packets is considered to be an intentional and J is penalized by decreasing its trust value by δ for each packet dropped. A tolerance level of τ_l is allowed to accommodate dynamic variation in channel conditions. If the trust value of node J falls below a threshold value Υ_u(upper-threshold), then I requests for a recommendation about that particular neighbor J. The evaluation time interval can be set accordingly, i.e. the duration can be short or long depending on the type of application in which the model is employed.

The upper and lower threshold values are just to facilitate the characterization of malicious activity of nodes. A higher lower threshold allows protocol to converge quickly, thus identifying malicious behavior. This may sometimes results into falsely ignoring genuine nodes . For a higher percentage of malicious nodes , HWMP-TX incurs higher losses , as it takes more time to converge. This behavior can be attributed to the optimistic nature of HWMP-TX protocol.

Algorithm 1 Trust evaluation

```
1: Carried out by each node I at the end of their TE_interval
2: for each neighbor J do
3:    if (β_ji > α_ji − (ε_l + τ_l)) then
4:       V_ij = u_ij + δ //good behavior
5:    else if (β_ji < α_ji − (ε_l + τ_l)) then
6:       V_ij = u_ij − δ //Suspicious behavior
7:       if (Vij < Υ_u) then
8:          requestRecommendation(J )
9:       end if
10:   else if (β_ji == α_ji − (ε_l + τ_l)) then
11:      V_ij = u_ij //expected behavior
12:   end if
13: end for
```

5.1.3 Trust Recommendation

Trust recommendation procedure shown in Algorithm 2, is reactive one carried out by a node I when the trust value of a neighbor J falls below Υ_u .

Algorithm 2 Trust recommendation

1: Executed by node I after receiving r recommendations
2: $\psi_{ij} = \frac{T_{ki}*T_{kj}+T_{li}*T_{lj}+....+T_{ri}*T_{rj}}{r}$
3: **if** $\psi_{ij} < \Upsilon_l$ **then**
4: M = True // Node I sets J status to malicious
5: **else if** $\psi_{ij} > \Upsilon_u$ **then**
6: Continue normal network operations
7: **else if** $\Upsilon_l < \psi_{ij} < \Upsilon_u$ **then**
8: Closely monitor J
9: **end if**

Nodes that receive a request for trust recommendation, check their respective neighbor list to verify the existence of J. If J exists in their neighbor list, it replies to the request sent by I with the current trust value of J in its list. Once, node I receives all the recommendations, it re-evaluates the trust value of J. If the revised trust value denoted by ψ_{ij}, falls below Υ_l, then node I assumes J to be malicious.

5.2 Trust Based Secure Routing (HWMP-TX)

The proposed trust model works in conjunction with HWMP to enable better route discovery process. It periodically evaluates the behavior of each of its neighbors by monitoring their forwarding behavior. It allows the routing protocol HWMP, to establish secure end-to-end routes by providing it with the observed trust values. The path selection process of HWMP-TX is shown in Table 3.

A source node O initiates a route discovery process by broadcasting a PREQ for a destination node D. An intermediate node I that receives a broadcasted PREQ, first verifies whether the trust value of the transmitter (For example, O in the first turn) is above a predefined threshold Υ_u. If the transmitter does not meet the desired trust requirements, PREQ's from such nodes are not processed further. This process is repeated by each intermediate node until the PREQ reaches destination or a node that has fairly fresh route to the destination. Finally, when the PREQ reaches the destination D, it too verifies the trust value of the transmitter, and selects a better route, before unicasting a PREP. The trust model ensures that the nodes included in the path, pass the basic trust acceptance criteria. Overall the route selection process is mainly driven by the airtime of a link and the trust model complements the path formation by ensuring that the selected nodes satisfy the basic acceptance criteria.

6 Security Analysis and Performance Evaluation

6.1 Security Analysis

6.1.1 Flooding Attack

An internal malicious node can generate any number of PREQ's requesting for paths to non-existent destinations. This attack can be easily handled by limiting the number of requests that a node can generate depending upon their reputation. HWMP-TX can naturally handle this kind of attack as the requests from a node are processed if and only if they satisfy the minimum trust criterion. As, HWMP-REX does not establish any lower bound on the reputation levels, a node can flood the network with fake requests.

6.1.2 Metric Manipulation Attack

The most common modification attack in a high throughput network is a metric manipulation attack. Malicious nodes can manipulate the metric field to include themselves in the selected path and later launch various packet dropping attacks. These attacks can be successfully launched before the nodes begin their monitoring process. Once, trust relationships are established, and nodes begin their monitoring process, the success percentage of these attacks falls drastically. In HWMP-REX and HWMP-TX, as nodes with lower reputation are avoided in path selection process, this kind of attack can be usually detected over time.

6.1.3 Wormhole Attack

Malicious can act in collusion to record packets at one end of the network and replay them at the other end. The main aim of this attack is to convince two far away nodes as neighbors. Once, a wormhole is established, the nodes can launch several packet dropping attacks. HWMP-REX fails to detect attacks from such colluded nodes as the watchdog does not guarantee reception at the receiver. HWMP-TX can identify such colluded nodes independently with the help of other nodes sharing neighborhood with such a malicious node and it can detect packet dropping attacks.

6.1.4 Blackhole Attack

Any malicious node's ultimate goal is to disrupt network services, and blackhole attack is the easiest and most straight forward among all the attacks. For a node to behave as a blackhole, first it has to become a part of the selected path. Hence, a blackhole attack is always launched in conjunction with other attacks such as, a metric manipulation attack. A node cannot behave as a blackhole for an extended period of time as the trust evaluation mechanisms of both HWMP-TX and HWMP-

Table 3: HWMP-TX path selection process

Executed at the source node *S* initiating Path Discovery process
1: Create a PREQ element similar to HWMP
2: Set the Metric field to 0
3: Broadcast the PREQ
Executed at the intermediate node J upon receipt of the PREQ
1: Check the PREQ-ID to avoid processing duplicate PREQ's
2: ***if*** $(duplicate)$ *then* Drop the PREQ return; ***else*** verify the trust value of the transmitter. // S in the first run
3: ***if*** $(TV_{Transmitter} < \Upsilon_u)$ *then* Drop the PREQ ***else*** Process the PREQ similar to HWMP
4: Update current link metric: Metric=currentLinkMetric + Metric.
6: ***if*** $(Route\ to\ source\ is\ available)$ *then* Unicast PREP Rebroadcast PREQ ***else*** Rebroadcast PREQ
Executed at the Destination node D upon receipt of PREQ
1: Verify the trust value of the transmitter to satisfy acceptance criteria
2: Include current link metric: Metric = currentMetric + Metric
3: Choose a path with the best metric.
4: Unicast the PREP.

REX can easily detect such attacks and avoid such nodes in future path selection process.

6.1.5 Fabrication Attack

Selfish nodes can fabricate messages to avoid consumption of their resources. For example, a node can fabricate a PERR message to inform the downstream nodes about an active link as broken. HWMP-REX inherently cannot handle such an attack as there is no way to distinguish between a genuine and fabricated PERR message. In HWMP-TX, for a node to maintain neighbor relations, it needs to keep its links active and this restricts a node from frequently generating fabricated messages.

7 Experimental Results

7.1 Simulation of Trust

We evaluate the performance of HWMP-REX and HWMP-TX by performing the following simulations on Omnet++ 4.2.1 discrete event simulator. We consider a backbone mesh network of 40 uniformly distributed mesh routers placed over the area of 2000 m^2. The transmission range of each mesh router is set to 100m. Each simulation is performed 10 times and the average results are presented. Mesh routers implement 802.11s MAC protocol with a channel data rate of 11mbps. Nodes uses CBR data traffic.

To begin with, we analyze the throughput achieved by HWMP-REX and HWMP-TX. Out of 40 mesh routers 20% of mesh routers (i.e. 8 nodes) exhibit malicious behavior. Malicious nodes are strategically selected in such a way that they become part of the network path. Figure 2 summarizes the performance of both the protocols. HWMP-REX achieves higher throughput during the initial stages of network activity. However as the simulation time progresses the throughput gradually falls below HWMP-TX. On the other hand, HWMP-TX achieves higher throughput as the life time of the network progresses . This is due to the fact that HWMP-REX assigns higher weighage to the resulting trust values in comparison to HWMP-TX. Since, any kind of malicious activity lowers the trust, thus increasing the virtual distance there by allowing HWMP-REX to select higher trusted paths over high throughput paths. But, HWMP-TX waits for an interval of time (When trust falls below higher threshold) before ignoring malicious nodes. HWMP-TX employs only airtime metric to select routes and trust is used to check whether the nodes meet the minimum trust criterion. Even though the lower threshold employed by HWMP-TX is 0.25 , this value does not have any impact on the achieved throughput. This is because the threshold values are just to facilitate the characterization

of malicious activity.

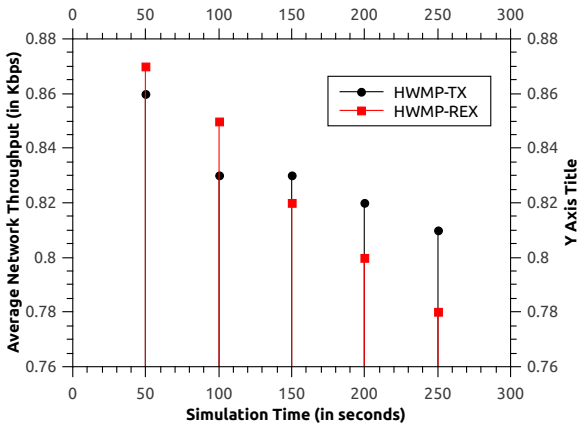

Figure 2: Throughput of HWMP-TX compared with HWMP-REX

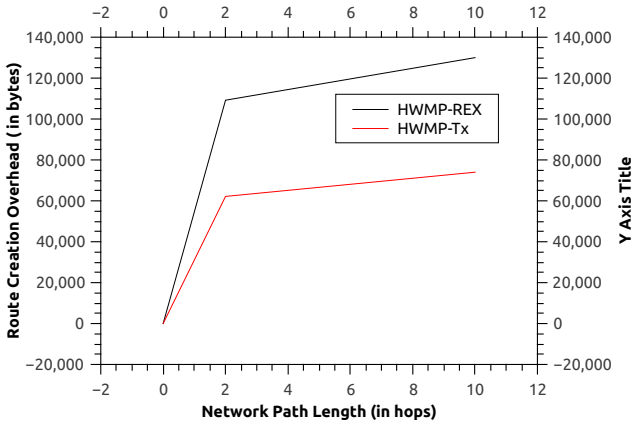

Figure 3: Overhead of HWMP-TX compared with HWMP-REX

A higher lower threshold allows protocol to converge quickly thus identifying malicious behavior. This may sometimes results into falsely ignoring genuine nodes. For a higher percentage of malicious nodes, HWMP-TX incurs higher losses, as it takes more time to converge. This behavior can be attributed to the optimistic nature of HWMP-TX protocol.

7.2 Route Creation Overhead

Next, we compute the route creation overhead of both the protocols. The route creation overhead is computed in accordance with theoretical results presented in [9]. The route creation rate per node is set to 1(λ =1) in our simulation. The average length of the route is varied between 2 to 10. The results are shown in Figure 3. The higher overhead of HWMP-REX can be attributed to increased size of PREQ. The PREQ packet employed by HWMP-REX needs to accommodate the reputation values and node addresses of each of it's neighbors. For an average of node degree 4, the packet size increases by 28 bytes (i.e.4*6 bytes per node address + 4*1 byte per reputation value). Since, HWMP-TX does not add any additional information to PREQ, its overhead remains same as HWMP. Figure 3 shows that the route creation overhead of HWMP-REX is relatively higher than HWMP-TX.

8 Discussion

Herein, we discuss the various factors that need to be accounted for comparing of both the frameworks. The comparison of both the protocols is presented in Table 4.

8.1 Path Fluctuations

Path fluctuations are frequent in HWMP-REX as it naturally prefers paths containing nodes with relatively higher reputation. The lower bounds established by HWMP-TX to tolerate transient changes in behavior thus preventing frequent switching of paths. Moreover, the paths selected by HWMP-TX perform better on average than HWMP-REX.

8.2 False Positives

False positive is a situation where a genuine is reported to be malicious. HWMP-REX directly does not exhibit such behavior, but penalizing and avoiding a good node from path selection is an indirect indication of false positive. Chances of arising such alarms are higher in HWMP-REX as it does not consider transient losses in the network. Frequent path switching is one of the indicators of false positives. On the other hand, HWMP-TX considers those packet losses and avoids frequent path fluctuations there by considerably lowering the probability of generating such false positives.

Table 4: Comparison of HWMP-REX and HWMP-TX

	HWMP-REX	HWMP-TX
Path Fluctuations	High	Low
False Positives	High	Low
False Negatives	Low	Low
Complexity	High	Low

8.3 False Negatives

False negative is a situation where a node is actually malicious and it is reported to be genuine. In HWMP-REX the watchdog module allows a node to ensure that its neighbor genuinely forwards the packets addressed to it. If the watchdog fails to detect any kind of malicious packet drop, then there is a chance of considering a malicious

node as genuine. But, as the failure of a watchdog is highly unlikely, false negatives are next to nil in HWMP-REX. In HWMP-TX, a malicious node can fake genuine behavior until it meets the established lower bounds on trust levels. Once, the trust value of a node falls below a predefined threshold, it cannot fake honest behavior. The monitoring mechanism of both the protocols ensure that a malicious node is never reported as genuine.

8.4 Complexity

HWMP-REX is more complex than HWMP-TX mainly due to the oversize of the RREQ. It also adds additional complexity to the processing of RREQ. Each node along the path to the destination appends the reputation of its neighbors along with their 6 byte addresses, thus increasing the overall size of the RREQ. Ignoring common neighbors and assuming average neighbor degree in a network to be 4, the additional overhead contributed by each node is 28 bytes.

9 Conclusion and Future Work

The performance requirements play a major role in modelling trust for a distributed network like WMN. The existing trust models for distributed networks are not directly employable and need to be significantly modified to meet the performance requirements of WMN. Therefore, we first modified an existing reputation framework, AODV-REX, specially tailored to WMN. We then proposed a complete trust model based on an alternate mechanism to employ trust in path selection process to improve the reliability and quality of selected paths. The proposed trust model allows a node to evaluate the behavior of its neighbors periodically. The experimental results of both the protocols confirm that HWMP-TX achieves better performance over existing models and also incurs less overhead. For future work, we plan to refine the established bounds to differentiate malicious behavior more accurately.

Acknowledgments

The authors gratefully acknowledge the anonymous reviewers for their valuable comments.

References

[1] A. Abdul-Rahman and S. Hailes, "A distributed trust model," in *Proceedings of the 1997 ACM Workshop on New Security Paradigms*, pp. 48–60, 1998.

[2] I. F. Akyildiz, X. Wang, and W. Wang, "Wireless mesh networks: A survey," *Computer Networks*, vol. 47, no. 4, pp. 445–487, 2005.

[3] M. Bahr, "Proposed routing for IEEE 802.11 s WLAN mesh networks," in *Proceedings of the 2nd Annual ACM International Workshop on Wireless Internet*, pp. 5, 2006.

[4] T. Clausen and P. Jacquet, *Optimized Link State Routing Protocol (OLSR),*, Technical Report, 2003.

[5] D. S. J. De Couto, D. Aguayo, J. Bicket, and R. Morris, "A high-throughput path metric for multi-hop wireless routing," *Wireless Networks*, vol. 11, no. 4, pp. 419–434, 2005.

[6] R. Draves, J. Padhye, and B. Zill, "Routing in multi-radio, multi-hop wireless mesh networks," in *Proceedings of the 10th Annual ACM International Conference on Mobile Computing and Networking*, pp. 114–128, 2004.

[7] T. Eissa, S. A. Razak, R. H. Khokhar, and N. Samian, "Trust-based routing mechanism in manet: design and implementation," *Mobile Networks and Applications*, vol. 18, no. 5, pp. 666–677, 2013.

[8] T. Ghosh, N. Pissinou, and K. Makki, "Collaborative trust-based secure routing against colluding malicious nodes in multi-hop ad hoc networks," in *29th Annual IEEE International Conference on Local Computer Networks*, pp. 224–231, 2004.

[9] P. Jacquet and L. Viennot, "Overhead in mobile adhoc network protocols," 2000.

[10] I. Khalil, S. Bagchi, and N. B. Shroff, "Liteworp: A lightweight countermeasure for the wormhole attack in multihop wireless networks," in *Proceedings of IEEE International Conference on Dependable Systems and Networks (DSN'05)*, pp. 612–621, 2005.

[11] C. E. Koksal and H. Balakrishnan, "Quality-aware routing metrics for time-varying wireless mesh networks," *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 11, pp. 1984–1994, 2006.

[12] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," in *Proceedings of the 6th Annual ACM International Conference on Mobile Computing and Networking*, pp. 255–265, 2000.

[13] R. Matam and S. Tripathy, "Wrsr: Wormhole-resistant secure routing for wireless mesh networks," *EURASIP Journal on Wireless Communications and Networking*, vol. 2013, no. 1, pp. 1–12, 2013.

[14] K. Meka, M. Virendra, and S. Upadhyaya, "Trust based routing decisions in mobile ad-hoc networks," in *Proceedings of the Workshop on Secure Knowledge Management (SKM'06)*, 2006.

[15] Working Group of the IEEE 802 Committee et al, "IEEE p802. 11s/d5. 0–draft standard for information technology–telecommunications and information exchange between systems–local and metropolitan area networks–part 11: Wireless lan medium access control (mac) and physical layer (phy) specifications–amendment 10: Mesh networking", 2010.

[16] F. Oliviero, L. Peluso, and S. P. Romano, "Refacing: An autonomic approach to network security based on multidimensional trustworthiness," *Computer Networks*, vol. 52, no. 14, pp. 2745–2763, 2008.

[17] F. Oliviero and S. P. Romano, "A reputation-based metric for secure routing in wireless mesh networks," in *IEEE Global Telecommunications Conference (GLOBECOM'08)*, pp. 1–5, 2008.

[18] S. Paris, C. Nita-Rotaru, F. Martignon, and A. Capone, "EFW: A cross-layer metric for reliable routing in wireless mesh networks with selfish participants," in *Proceedings of IEEE INFOCOM*, pp. 576–580, 2011.

[19] C. Perkins, E. Belding-Royer, and S. Das, *Ad Hoc On-demand Distance Vector (AODV) Routing*, Technical Report, 2003.

[20] K. Sanzgiri, B. Dahill, B. N. Levine, C. Shields, and E. M. B. Royer, "A secure routing protocol for ad hoc networks," in *Proceedings of 10th IEEE International Conference on Network Protocols*, pp. 78–87, 2002.

[21] P. Subhash and S. Ramachandram, "Preventing wormholes in multi-hop wireless mesh networks," in *2013 Third International Conference on Advanced Computing and Communication Technologies (ACCT'13)*, pp. 293–300, 2013.

[22] A. P. Subramanian, M. M. Buddhikot, and S. Miller, "Interference aware routing in multi-radio wireless mesh networks," in *2nd IEEE Workshop on Wireless Mesh Networks (WiMesh'06)*, pp. 55–63, 2006.

[23] S. Tan, X. Li, and Q. Dong, "Trust based routing mechanism for securing oslr-based manet," *Ad Hoc Networks*, vol. 30, pp. 84–98, 2015.

[24] Z. Yan, P. Zhang, and T. Virtanen, "Trust evaluation based security solution in ad hoc networks," in *Proceedings of the Seventh Nordic Workshop on Secure IT Systems*, vol. 14, 2003.

[25] Y. Yang, J. Wang, and R. Kravets, "Designing routing metrics for mesh networks," in *IEEE Workshop on Wireless Mesh Networks (WiMesh'05)*, 2005.

[26] P. W. Yau, C. J. Mitchell, et al., "2HARP: A secure routing protocol for mobile ad hoc networks," 2015. (`https://pure.royalholloway.ac.uk/portal/files/4624400/2asrpf.pdf`)

P. Subhash received his M.Tech degree in Software Engineering from Jawaharlal Nehru Technological University Hyderabad, India in 2008. He is currently working towards his Ph.D degree in Wireless Mesh Network Security at Jawaharlal Nehru Technological University Hyderabad, India. His current research interest includes wireless network security and Peer-to-Peer Networking.

S. Ramachandram received the M.Tech degree from Osmania University, Hyderabad, India, in 1985, and Ph.D. degree in Computer Science and Engineering, Osmania University, Hyderabad, India in 2005. Currently he is a professor at Osmania University, Hyderabad, India. His research interests include Mobile Computing, Network Security and Grid Computing.