TEAM: Trust Enhanced Security Architecture for Mobile Ad-hoc Networks

Venkat Balakrishnan, Vijay Varadharajan, Uday Tupakula, and Phillip Lucas

Information and Networked System Security (INSS) Research Group
Department of Computing, Macquarie University
Sydney, Australia
{venkat, vijay, uday, philipl}@ics.mq.edu.au

Abstract — Security is paramount in Mobile Ad-hoc Networks (MANET) as they are not conducive to centralized trusted authorities. Several solutions have been proposed for MANET in the areas of key management, secure routing, nodal cooperation, and trust management. Nevertheless, MANET lacks a unified architecture to take advantage of the deployed security models. In this paper, we propose Trust Enhanced security Architecture for MANET (TEAM), in which a trust model is overlaid on the following security models - key management mechanism, secure routing protocol, and cooperation model. We briefly present the operation of our architecture and then we detail the system operation of our novel trust and cooperation model, which we call as Secure MANET Routing with Trust Intrigue (SMRTI) and fellowship respectively. SMRTI captures the evidence of trustworthiness for other nodes from the security models, and in return assists them to make better security decisions. Unlike related trust models, SMRTI captures recommendations in such a way that it eliminates both free-riding and honest-elicitation problems. In comparison with related cooperation models, fellowship model defends against both flooding and packet drop attacks. It can efficiently identify and isolate both malicious and selfish nodes that fail to share the communication channel or forward packets for other nodes. Furthermore, our models do not rely on any centralized authority or tamper-proof hardware. Simulation results confirm that our models enhance the performance of TEAM.

I. INTRODUCTION

A mobile ad hoc network (MANET) is a self-configuring network in which nodes rely on intermediate nodes to establish multi-hop communications. It is difficult to secure these networks as they are not conducive to centralised authorities. Further, security solutions from wired networks are not directly portable to ad hoc networks for reasons such as sporadic wireless communication, dynamically changing topology, and constrained battery energy.

Since multi-hop communications between any nodes is reliant on intermediary nodes, it is apparent that the security of higher layer protocols is conditioned by the security of communication path. Secure routing protocols have been proposed [1, 2] to discover secure paths between communicating nodes. These protocols achieve secure routing by authenticating the intermediary nodes, and validating path integrity. For this reason, each node is assumed to share a secret with every other node in the network. Nodes protect their communications by channelling the traffic only through the secure path. Traditional cryptographic mechanism may also be used to defend against eavesdropping.

As secure routing protocols are not designed to guarantee the availability of network, they are extremely vulnerable to attacks such as flooding and packet drop attacks. Although solutions have been proposed [3, 4] to induce cooperation among nodes, they fail to counteract flooding attacks. This is because they do not consider the behavioural patterns of nodes, and hence overlook to measure the trustworthiness for nodes. Recently, reputation and trust models have been proposed [5, 6] to evaluate the trustworthiness of nodes. However, these models introduce additional problems and modify basic routing operations in order to collect evidence of trustworthiness. Therefore, recommendations in these trust models are prone to issues such as honest-elicitation\(^1\) and free-riding\(^2\). In general, these models utilize trust decisions only for the purpose of choosing trustworthy routes (depending on the collected evidence), rather than extending the trust decisions to enhance the security of key management mechanism [7-9]. The later is so required in ad hoc networks, as nodes are prone to capture and compromise. In other words, it is an apparent requirement for the key management mechanism to consider the behaviour of nodes, so that it can dynamically exclude both internal attackers and compromised nodes from key refresh list. In summary, it is evident that the security solutions proposed for mobile ad hoc networks are disparate and prone to problems.

All the above motivated us to propose a Trust Enhanced security Architecture for MANET (TEAM), in which a trust model is overlaid on other security models such as key management, secure routing, and cooperation model to enhance the network security. In our architecture, the trust model is designed to capture the evidence of trustworthiness for other nodes from the key management, secure routing, and cooperation model without introducing further issues such as honest-elicitation, free-riding, and recommender’s bias. The trust model enhances the security decisions of the above security models depending on the predefined policies and collected evidence. The secure routing protocol is utilized to

---

\(^1\) A node is subject to honest-elicitation, when it forwards a high recommendation for a malicious node in order to avoid itself from being labelled with a low recommendation by the malicious node. A malicious node may also exhibit honest-elicitation by forwarding low recommendations for benign nodes, or high recommendations for colluding malicious nodes.

\(^2\) A node is subject to free-riding when it accepts recommendations from other nodes, but fails to reciprocate with recommendations when requested by them.

1-4244-1230-7/07/$25.00 © 2007 IEEE 182

ICON 2007

Authorized licensed use limited to: MACQUARIE UNIV. Downloaded on February 4, 2009 at 21:21 from IEEE Xplore. Restrictions apply.
discover secure paths and to protect communications through the secret associations established and maintained by the key management mechanism. In our architecture, the secure routing protocol forwards evidence for fabrication and modification attacks to the trust model, and in return takes advantage of the trust model’s feedback to make better routing decisions. Although the key management mechanism does not forward any evidence to the trust model, it relies on the trust model’s feedback to dynamically manage the keys. The cooperation model in our architecture differs from related models [3, 4] by defending against both flooding and packet drop attacks. Similar to other security models, it forwards evidence to the trust model, and takes advantage of the trust model’s feedback to decide whether to forward a packet on behalf of other nodes. In summary, the proposed Trust Enhanced security Architecture for MANET (TEAM) extends our previous work, Trust Integrated Cooperation Architecture [10] so that it not only assists security models such as key management, secure routing, and cooperation model to make better decisions, but also enables them to handle the dynamic behaviours of nodes. Hence, Secure MANET Routing with Trust Intrigue (SMRTI) [11, 12], and fellowship [14, 15] are chosen for trust and cooperation models respectively.

The paper is organized as follows. In Section 2, we discuss the characteristics and limitations of well-known related models. In Section 3, we outline the context, and then we present the overview of our architecture. Section 4 details the operation of SMRTI and Section 5 describes the operation of fellowship model within the context of our architecture. We then briefly discuss the simulation results to demonstrate the properties of both SMRTI and fellowship in Section 6. Finally, Section 7 gives some concluding remarks.

II. RELATED WORK

In the following, we briefly present few well-known secure routing protocol and key management mechanisms, and then focus on few well-reviewed cooperation models. Finally, we conclude our discussion with few well-analysed reputation and trust models.

Ariadne [1] employs broadcast and hop-by-hop authentication, while Secure Routing Protocol (SRP) [2] performs end-to-end authentication through symmetric key based mechanism. These secure routing protocols are primarily designed to discover secure paths, and therefore they fail to defend against both flooding and packet drop attacks.

Zhou and Hass [7] introduce two types of nodes known as server and combiner apart from the normal nodes (called as client nodes) to play the role of Certificate Authority (CA). They deploy threshold based cryptography to establish the services of CA. In [8], Luo et al. replaced the above-mentioned specialized server nodes by distributing the capability of CA to all nodes. Distributed Key Pre-distribution Scheme (DKPS) [9] is a fully distributed and self-organized key pre-distribution which does not rely on any infrastructure support. Nevertheless, these approaches are prone to refresh keys with malicious and compromised nodes.

Nuglets [3] enforces nodes to cooperate by using virtual currencies. In spite of efficiency, the usage of tamper-resistant hardware makes Nuglets unattractive. Alternatively, Sprite [4] uses incentives to motivate cooperation among selfish nodes. Sprite is non-generic as it relies on a central authority to manage incentives and also fails to address malicious nodes.

In [5], Liu and Yang collect reputations from recommenders and combine them to update the reputation for recommended node. The main drawback of the model is that the malicious nodes are assumed to recommend truthfully irrespective of their misbehaviours. Yan Lindsay et al. [6] proposed a trust model based on information theory for improving the security of ad hoc routing protocols. Similar to other models, they monitor other nodes and exchange recommendations with other nodes in a distributed manner for establishing trust relationships. It is apparent from the discussion that the related trust models fail to address the issues associated with recommendations such as the bias of a recommender, honest-elicitance and free-riding problems. Also, they fail to render feedback to enhance the decisions of security models such as key management, secure routing, and cooperation model.

III. TRUST ENHANCED SECURITY ARCHITECTURE

In this paper, we explore TEAM through the Dynamic Source Routing (DSR) protocol. The nodes rely on passive monitoring to capture evidence for the benign and malicious behaviours of neighbours. We attribute flooding, packet dropping, fabricating and modifying behaviours as malicious behaviours.

As shown in Fig. 1, the secure routing protocol and key management mechanism are used to discover secure paths and protect subsequent communications. In sequence, the fellowship model is used to defend against both flooding and packet drop attacks. Our architecture integrates these security models through SMRTI, which asynchronously collects evidence of trustworthiness for other nodes from these models. Otherwise, SMRTI synchronously responds to the requests received from the security models. This in turn enables security models to react accordingly to the behavioural changes of other nodes. Next, we briefly detail the interactions among the security models and SMRTI within a node.

Let us consider the path \( S \rightarrow O \rightarrow X \rightarrow N \rightarrow C \rightarrow D \) in which \( S \) is the source and \( D \) is the destination for the communication flow. Nodes \( O \), \( X \), \( N \) and \( C \) are the intermediate nodes that form the path from \( S \) to \( D \). Node \( S \)
initially checks its route cache for a route to D, whenever it wishes to send a data packet to D. On finding one or more routes, DSR passes the route(s) to SMRTI in order to evaluate their trustworthiness. The trust evaluation for a route is performed by evaluating the trustworthiness for all nodes in the route, except for the evaluating node (i.e., S). The route with highest level of trustworthiness is chosen for the communication flow and passed back to DSR, provided there is more than one trustworthy route for D. DSR then requests secure routing protocol to incorporate necessary security services through the cryptographic suite and shared secrets managed by key management mechanism. Alternatively, if all the routes are untrustworthy, or there is no available route to D, then SMRTI responds back to DSR with a decision to initiate a new route discovery cycle to D.

Let us now consider the role of our architecture in an event (route request, route reply, error report, or data flow) at one of the intermediate nodes O, X, N, and C. To begin with, the fellowship model at every intermediate node checks the transmission-rate of previous-hop. Given the previous-hop’s transmission-rate is at least equal to the flooding rate defined by transmission-threshold $\tau$, the fellowship model discards the packet and forwards the evidence for malicious behaviour to SMRTI. Otherwise, it requests SMRTI to evaluate trustworthiness for the previous-hop. This is in accordance with the expectation that the packet is not exposed to malicious behaviour only if the previous-hop is trustworthy. Fellowship model then passes the packet to secure routing protocol to incorporate necessary security services. If the later fails to authenticate the intermediate nodes listed in route or unable to verify the discovered path’s integrity, it then forwards the evidence for fabrication or modification respectively to SMRTI. Otherwise, the secure routing protocol requests SMRTI to evaluate trustworthiness for the packet. This is for the reason that intermediate nodes forward packet only for the sake of source S and destination D. In addition, SMRTI evaluates trustworthiness for the route contained in the packet, and inserts the route into DSR’s route cache only if the route is trustworthy. Once secure routing protocol confirms that the packet is trustworthy, it applies the required security services to the packet and then passes the packet back to the fellowship model. Now the fellowship model requests SMRTI to evaluate trustworthiness for the next-hop. This is to meet with the expectation that the packet will reach the destination D without being exposed to malicious behaviour, only if the next-hop is trustworthy. In the case of route request event, the trust evaluation for next-hop is skipped as the next-hop is unknown due to the broadcast nature of route request. Nevertheless, if the next-hop drops the packet, the fellowship model investigates its transmission-rate and contention for the transmission channel before forwarding the evidence for packet drop to SMRTI. However, if the next-hop forwards the packet without performing any malicious behaviour then the fellowship model forwards the evidence for benign behaviour to SMRTI.

Similarly, the fellowship model at D checks its previous-hop for flooding before requesting SMRTI to evaluate trustworthiness for the previous-hop. It then passes the packet to secure routing protocol which first authenticates and verifies the packet, and then evaluates trustworthiness for the packet and route through SMRTI.

The sequence of operation explained above for source S, destination D, and intermediate nodes holds only for the network which is extremely exposed to malicious nodes. In conditions where the degree of maliciousness is lower, few of the trust evaluations can be skipped.

IV. OVERLAY TRUST MODEL - SMRTI

SMRTI assists the security models in making decisions for the following contexts such as whether to – accept or reject a route from a route discovery, record or ignore a route from a forwarded packet, to forward or discard a packet, to forward a packet for a previous-hop, to send a packet to a next-hop, refresh or revoke the key for a node, and which route to choose for the communication. The decision in each context depends on the corresponding trust evaluation. In turn, trust evaluations are based on the direct and recommended trust held for one or more nodes involved in the context. A node’s direct trust is based on the evidence captured by its security models during one-to-one experiences with the other node. The recommended trust is based on the recommendations derived for a node.

A. Trust Evaluation

Let us now consider the trust evaluation for – a node, a packet, and a route. Assume that every node’s direct and recommended trust for all other nodes is initialized to the default threshold value, threshold-limit $\Delta$. A positive trust evaluation for a node (packet or route) depends on whether the computed trustworthiness for the node (packet or route) is at least $\Delta$.

Node ‘$i$’ computes trustworthiness $(T_{Node}(t_{a\rightarrow i}))$ for node ‘$j$’ at time $t_{a+1}$ using its direct $(DT_{Node}(t_{a}))$ and recommended $(RT_{Node}(t_{a}))$ trusts for ‘$j$’, as given in (1). We give higher priority to direct trust than for the recommended trust, as personal experiences take higher precedence over the recommendations received from others, which is given by ‘$\alpha$’ in (1).

$$T_{Node}(t_{a+1}) = [\alpha \cdot DT_{Node}(t_{a})] + [(1-\alpha) \cdot RT_{Node}(t_{a})]$$

$$0 < \alpha < 1; \quad t_{a+1} > t_{a} \quad (1)$$

Trustworthiness $(T_{Packet}(t_{a\rightarrow j}))$ for a packet ‘$k$’ at node ‘$i$’ is computed from the trustworthiness held for both the packet’s source $(T_{Node}_{Src}(t_{a}))$ and destination $(T_{Node}_{Dest}(t_{a}))$, which is given in (2).

$$T_{Packet}(t_{a+1}) = [\beta \cdot T_{Node}_{Src}(t_{a})] + [(1-\beta) \cdot T_{Node}_{Dest}(t_{a})]$$

$$0 < \beta < 1 \quad (2)$$

Finally, trustworthiness $(T_{Route}(t_{a\rightarrow i}))$ for a route ‘$r$’ at node ‘$i$’ is computed from the trustworthiness held for all the nodes $(T_{Node}(t_{a}))$ positioned in the path, excluding node ‘$i$’, which is given in (3).

$$T_{Route}(t_{a+1}) = \sum_{j \in r \land i \neq j} T_{Node}(t_{a}); \sum_{j \in r \land i \neq j} \lambda = 1 \quad (3)$$
B. Direct Trust

A node’s direct trust for another node is defined as the trustworthiness computed for the other node from the evidence captured during the one-to-one interactions. The evidence is attributed either to a positive \(\{\text{pos}(\text{event})\}\) or a negative value \(\{\text{neg}(\text{action, event})\}\), depending on whether the other node’s behaviour is either malicious or benign respectively. The magnitude of the positive value is proportional to the type of event (route request, route reply, route error or data flow). In contrast, the magnitude of negative value is a function of both the type of event and malicious behaviour (flooding, packet dropping, modification of route sequence number, addition or deletion of routes, and fabrication). Further, the malicious node is excluded from the corresponding communication flow until the completion of flow, regardless of its trustworthiness.

As given in (4), node ‘i’ revises its existing direct trust for node ‘j’, from the evaluated evidence [i.e., pos (event), or neg(action, event)]. After the computation, the revised direct trust ‘\(\text{DT}_{i\text{Node}}(t_{a+i})\)’ becomes the existing direct trust for future computation. Similar to [6], trust is measured in the range of [-1, +1] as discrete trust values can only provide a small set of possible trust values, while trust in mobile ad hoc networks evolves continuously.

\[
\text{DT}_{i\text{Node}}(t_{a+i}) = \begin{cases} 
\text{min} +1, & [\text{DT}_{i\text{Node}}(t_a) + \text{pos}(\text{event})], \text{ ‘i’ is benign} \\
\text{max} -1, & [\text{DT}_{i\text{Node}}(t_a) - \text{neg}(\text{action, event})], \text{ ‘i’ misbehaves} 
\end{cases}
\]

C. Recommended Trust

For ease of explanation, the node that provides a recommendation is referred as recommender and the recommended node is referred as recommendee. In related models [5, 6], recommendations are communicated among nodes by disseminating explicit data packets or additional headers. In these models, the notion of disseminating recommendations corrects the trust decisions for following reasons. First, they lack well-analyzed approaches to determine the bias of a recommender. Second, they fail to investigate whether the recommender exhibits free-riding or honest-elicitation behaviours. Even when these models do attempt to address these problems, they lack well-defined approaches to completely defend against them. In addition, disseminating recommendations increases overhead and consequently degrades network performance.

In contrast, recommendations in SMRTI are derived for a recommendee using the route contained in a packet. SMRTI deduces a node’s intention to forward or discard an upstream packet received from its previous-hop, as the node’s opinion for its previous-hop. It then derives the deduced opinion as the node’s recommendation for its previous-hop. Since recommendations are derived from the route of a received packet, both the route and packet are evaluated as detailed in Section IV.A before deriving recommendations. In addition, recommendations are derived only once for a communication flow during the data flow event in order to avoid the influence of malicious routes.

Consider the scenario where node X unicasts a packet to node N, which contains the route S \(\rightarrow\) O \(\rightarrow\) X \(\rightarrow\) N \(\rightarrow\) C \(\rightarrow\) D. Node N will forward the received packet, only if the packet is trustworthy. N derives X’s willingness to forward the packet on behalf of O, as X’s recommendation for O. Similarly, N derives O’s willingness to forward the packet on behalf of S, as O’s recommendation for S. The process of deriving recommendations terminates at S as there is no previous-hop for S.

We now consider the recommendation derived from X (recommender) for O (recommendee) by N to detail the computation. N computes its trustworthiness for X according to (1). A positive or negative value is assigned for the derived recommendation depending on whether the trustworthiness held for X is at least equal to ‘\(\Delta\)’. This demonstrates N’s view on the recommendation derived from X for O. This positive (or negative) value is also identical with the positive (or negative) values assigned for recommendations derived from other nodes. In other words, the above operation fails to present the fact that the trustworthiness held by N for X need not be the same as the trustworthiness held for other nodes. Hence, the positive (or negative) value representing the recommendation derived from X for O is scaled by the trustworthiness held by N for X. The scaling affirms that the recommendation is proportional to the trustworthiness held by N for X. Finally, N revises its existing recommended trust for O by integrating the recently computed positive (or negative) value for O. The same operation is then repeated for the recommendation derived from O for S. Equation (5) summarizes the operations in which \(\text{RT}_{i\text{Node}}(t_{a+i})\) is the revised recommendation for node ‘j’ by node ‘i’.

\[
\text{RT}_{i\text{Node}}(t_{a+i}) = \begin{cases} 
\text{min} +1, & [\text{RT}_{i\text{Node}}(t_a) + \text{pos}(\text{event})]/\text{if} T_{i\text{Node}}(t_a) \geq \Delta \\
\text{max} -1, & [\text{RT}_{i\text{Node}}(t_a) - \text{neg}(\text{action, event})]/\text{if} T_{i\text{Node}}(t_a) < \Delta 
\end{cases}
\]

In summary, the proposed approach prevents the opinion of a node from being corrupted by the recommender, and this in turn enforces the node to rely on its opinion. Hence, it better resolves the issues concerned with the recommender’s bias. Since the recommenders do not forward their opinions, the proposed approach prevents the recommenders from exhibiting both honest-elicitation and free-riding behaviours.

V. OBLIGATION-BASED COOPERATION MODEL - FELLOWSHIP

Fellowship uses an obligation-based approach to defend against both flooding and packet drop attacks. This enables sharing of the communication channel and forwarding of packets for other nodes in turn to receive the same network services from them.

A. Attacker Model

Unlike related models [3, 4], the fellowship model defends against both malicious and selfish nodes. The nodes that drain the resources or obstruct the communications of other nodes are known as malicious nodes. Selfish nodes exploit the self-organized characteristic of ad hoc networks in order to retain their resources or use their resources to override other nodes.
Selfish nodes are unique to mobile ad hoc networks because of the prevailing heterogeneity and the resource constraints among the nodes. Although the intention of selfish nodes is different from malicious nodes, we classify their behaviours as malicious.

B. System Operation

Fellowship model defends against both flooding and packet drop attacks by passing an incoming packet to – rate-limited, enforced, and restoration components.

The rate-limitation component monitors the channel usage of the previous-hop at regular intervals of time. The previous-hop is presumed to be flooding, if its transmission-rate exceeds the pre-defined transmission-threshold (T) within a given interval (i.e., if the previous-hop fails to comply with the obligation of sharing the communication channel). Rate-limitation discards the current and subsequent packets of the previous-hop, and in parallel forwards the evidence of flooding to SMRTI. The rate-limitation remains in this state until the transmission-rate of the previous-hop is limited to ‘T’. This defends against flooding attack at the point of origin. Alternatively, if the channel usage is within ‘T’, then the rate-limitation queries SMRTI to evaluate trustworthiness for the previous-hop. The rate-limitation then delivers the packet to the secure routing protocol for applying required security services, given that the previous-hop is trustworthy.

As long as the next-hop is trustworthy, the enforcement component advances the packet received from secure routing protocol to the restoration component, otherwise it discards the packet. Recall that the enforcement component confirms the next-hop’s trustworthiness by querying SMRTI. The untrustworthy previous-hop and next-hop can improve their trustworthiness only by exhibiting consistent benign behaviour in future, i.e. by forwarding unmodified packets within ‘T’.

However, if the untrustworthy nodes continue to exhibit persistent malicious behaviour, then they will remain isolated from the network.

Finally, restoration component makes the best possible effort to forward the packet to the next-hop. Prior to the packet propagation, it checks the transmission buffer queue, transmission-rate and communication channel to deduce the congestion and contention level. If the restoration component has to drop the packet due to unforeseen conditions such as congestions or contentions, it then passes on evidence to SMRTI in favour of the previous-hop.

It is important to note that the architecture at every node conceals its trust values from being comprehended by other nodes. This in turn enforces the selfish nodes to comply with the architecture; otherwise they are at the risk of being isolated from the network like the malicious nodes.

VI. SIMULATION RESULTS

We have used NS-2 simulator for analysing TEAM, in which we have evaluated only SMRTI and fellowship model in the absence of secure routing and key management to study their performance against modification, flooding, and packet drop attacks. The nodes that do not have SMRTI and fellowship model enabled are called as DSR nodes. The nodes that deploy SMRTI and fellowship model are known as TEAM nodes. The nodes that perform one of the attacks – modification, flooding, or packet drop attacks are called as malicious nodes. Simulation parameters are summarized in Table 1.

Table 1 - Simulation Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total simulation time</td>
<td>300s</td>
</tr>
<tr>
<td>Total number of nodes</td>
<td>100</td>
</tr>
<tr>
<td>Maximum velocity</td>
<td>20m/s</td>
</tr>
<tr>
<td>Pause time</td>
<td>10s</td>
</tr>
<tr>
<td>Simulation area</td>
<td>1200x1200m²</td>
</tr>
<tr>
<td>Total CBR connections</td>
<td>20</td>
</tr>
<tr>
<td>Threshold-limit (β)</td>
<td>0.50</td>
</tr>
<tr>
<td>Transmission-threshold (T)</td>
<td>3</td>
</tr>
</tbody>
</table>

The performance of TEAM and DSR nodes are compared against varying proportions of malicious nodes. Packet Delivery Ratio (PDR) is the evaluated performance metric, in which PDR is defined as the average ratio of total number of CBR data packets received by destination to the total number of CBR packets sent by source in a communication flow.
As shown in Fig. 2(a), TEAM nodes perform better than DSR nodes due to following reasons – accepting packets only from trustworthy previous-hops, forwarding packets only to trustworthy next-hops, propagating only trustworthy packets, and using only trustworthy routes. The result confirms that SMRTI enables TEAM nodes to establish valid routes, despite the increasing proportion of malicious nodes. Fig. 2(a) confirms that TEAM nodes do not incur additional overhead in the absence of malicious nodes.

From Fig. 2(b), it is evident that TEAM nodes exhibit improved performance in comparison with DSR nodes. However, in the presence of 90% packet dropping nodes, the performance of TEAM nodes is reduced significantly when compared with DSR nodes. This is due to the increased route discoveries, which results from the decision to exclude routes that contain packet dropping nodes.

Unlike Fig. 2(a) and 2(b), Fig. 3(c) shows the performance of flooding nodes against TEAM and DSR nodes. Flooding nodes perform better in the presence of DSR nodes. Alternatively, their performance is reduced against TEAM nodes due to the capacity of fellowship model to defend against flooding attack at the point of origin. This not only restricts the propagation of flooded packets but also drains the resources of flooding nodes.

VII. CONCLUSION

In this paper, we have presented our Trust Enhanced security Architecture for MANET (TEAM). In TEAM, we have successfully detailed the integration of security models (key management, secure routing, and cooperation model) with the trust model to enhance the network security. We have then demonstrated the deployment of Secure MANET Routing Trust Intrigue (SMRTI) and fellowship model in TEAM to achieve the functionality of trust and cooperation models respectively. In comparison with related models, SMRTI captures recommendation by eliminating both honest-elicitaiton and free-riding problems. Alternatively, fellowship model defends flooding attack at the point of origin and excludes packet drop attacks in the discovered secure path. Simulation results demonstrate the effectiveness of SMRTI and fellowship in TEAM. In future, we anticipate analysing TEAM by conducting detailed simulations involving trust and all security models.

REFERENCES


