IACSIT International Journal of Engineering and Technology Vol.1,No.5,December,2009
ISSN: 1793-8236

A Novel security framework for protecting Network Layer operations in MANET

N.Jaisankar, K.Durai Swamy

***Abstract*—The important security issue in mobile ad hoc networks is to protect the routing layer from malicious attacks. A unified security solution for such networks is applied to protect both routing and data forwarding operations in the routing layer. In this paper the proposed model does not apply the cryptographic primitives on the routing messages This model protects the network by detecting and isolating the malicious nodes. In this proposed model, every node is monitoring other nearest neighboring nodes. A novel recognition strategy is applied to decrease its overhead as time evolves. In the proposed model information cross-validation is used to protect the network in a self-organized manner. Through both analysis and simulation results, the effectiveness of proposed model in a MANET environment is demonstrated.**

Index Terms—**Mobile ad hoc network, network-layer security, malicious nodes**

I. Introduction

Mobile ad hoc network (MANET) is a type of wireless ad hoc network, and is a self-configuring network of mobile devices connected by any number of wireless links. Every device in a MANET is also a router because it is required to forward traffic unrelated to its own use. Each MANET device is free to move independently, in any arbitrary direction, and thus each device will potentially change its links to other devices on a regular basis. Such networks extend the limited wireless transmission range of each node by multihop packet forwarding. Security is one crucial requirement for these mission-critical applications. In particular, in MANET, any node may compromise the routing protocol functionality by disrupting the route discovery process.

In this paper, an important security issue is tackled in ad hoc networks, namely the protection of their network-layer operations from malicious attacks. Without appropriate protection, the malicious nodes can readily function as routers
and prevent the network from correctly delivering the packets. For example, the malicious nodes can announce incorrect routing updates which are then propagated in the network, or drop all the packets passing through them. A proposed model is used to protect both routing and packet forwarding together. The research directions towards security in MANETs are still at their infancy.

Manuscript received on June 1, 2009.
N.Jaisankar is with School of Computing Sceinces, VIT University, Vellore-14, India
Prof. K.Durai swamy is with KSR College of Technology, Tiruchengodu, India.

Security issues arise in many different areas including physical security, key management, routing and intrusion detection, many of which are vital to a functional MANET. Due to their particular architecture, ad-hoc networks are more easily attacked than wired network. There are two kinds of attacks: the passive attacks and the active attacks. A passive attack does not disrupt the operation of the protocol, but tries to discover valuable information by listening to traffic. Instead, an active attack injects arbitrary packets and tries to disrupt the operation of the protocol in order to limit availability, gain authentication, or attract packets destined to other nodes.

The routing protocols in MANET are quite insecure because attackers can easily obtain information about network topology. Indeed in AODV and DSR protocols, the route discovery packets are carried in clear text. So a malicious node can discover the network structure just by analyzing this kind of packets and may be able to determine the role of each node in the network. With all these information more serious attacks can be performed in order to disturb the network operation by isolate important nodes, etc. The attacks in modification and impersonation are:

One of the simplest ways for a malicious node to disturb the good operation of an ad-hoc network is to announce better routes (to reach other nodes or just a specific one) than the other nodes.

These attacks are called spoofing since the malicious node hide its real IP address or MAC address and uses another one. As current ad-hoc routing protocols like AODV and DSR do not authenticate source IP address, a malicious node can launch many attacks by using spoofing. For example, a hacker can create loops in the network to isolate a node from the remainder of the network. To do this, the hacker just has to take IP address of other node in the network and then use them to announce new route (with smallest metric) to the others nodes. By doing this, he can easily modify the network topology as he wants.

- Redirection by changing the route sequence number
- Redirection with modified hop count (specific to AODV protocol)
- Denial Of Service (DOS) attacks with modified source routes
- Attacks using fabrication

As a solution for these kinds of attacks, a routing layer security solution has been provided in ad hoc networks. In this paper, developing a IDS security framework has been proposed. This IDS security framework involves:

1. Detection of malicious nodes
2. Isolation of malicious nodes
3. Prevention

The paper is organized as follows. Section 2 discusses the related work done in the same area. Section 3 presents the overview of the proposed model. Performance Evaluation and simulation results are given in section 4 and the conclusion is given in section 5.

II. PREVIOUS WORK

Marti and others [1] proposed watchdog that monitors a node based on overhearing the channel. The collaborative monitoring mechanism in proposed model differs from Watchdog in two aspects. First, while Watchdog focuses on packet forwarding misbehavior, proposed model aims at monitoring both routing and packet forwarding activities of each node. Second, proposed model exploits local collaboration to address the inherent imperfectness of the information gathered by channel overhearing.

Hubaux et al. [2] proposed a self-organized public-key infrastructure for ad hoc networks, the idea of which was similar to pretty good privacy (PGP). In this infrastructure, the certificate of each node is issued by other nodes, and the certificate chain is used to verify a given certificate. However, as inherited from the PGP trust model, this design is intolerant of compromised nodes which, unfortunately, are an unavoidable security threat in mobile ad hoc networks. Perhaps the most relevant work to proposed model is the localized certification service proposed by Kong et al. [3]. The certificate renewal process in proposed model is similar to this scheme.

Hu et al. [4] proposed the Ariadne protocol, which uses one-way key chains and source-destination pairwise keys to protect the DSR routing protocol. The same authors [5] also proposed the secure efficient distance vector protocol (SEAD) to secure the destination sequenced distance vector routing (DSDV) protocol based on one-way hash chains. Papadimitratos and Haas [6] proposed the secure Routing protocol (SRP) protocol which relied on the secret association between source and destination to protect the source routing messages.

Sanzgiri et al. [7] presented the Authenticated Routing for Adhoc networks (ARAN) protocol which exploits asymmetric cryptography to authenticate the routing messages based on each node's public-key certificate, distributed by a central trusted server. Zapata and Asokan [8] proposed the secure ad-hoc on-demand distance vector (SAODV) protocol which uses both one-way hash chains and data signatures to secure the AODV routing protocol.

CONFIDANT [16] protocol (Cooperation of Nodes; Fairness In Dynamic Adhoc Networks) as proposed by Buchegger et al extends the concepts of watchdog and pathrater. In this mechanism, misbehaving nodes are not only excluded from\ forwarding route replies, but also from sending their own route request. The scheme includes a trust manager to evaluate the level of trust of alert reports and a reputation system to rate each node. The reports from trusted sources are only processed by the nodes. However, it is not clear how fast the trust level can be adjusted for a compromised node especially if it has a high trust level initially.

All these protocols take the proactive approach and prevent malicious attacks by protecting the routing messages through cryptographic primitives. They either assume some kind of a priori secret association or key exchange between the nodes, or assume the existence of a centralized trusted server in the network.

The monitoring result at each individual node does not take effect until its neighbors has reached a consensus. The detection performance is, thus, significantly improved. On the contrary, proposed method takes the reactive approach by detecting and reacting to malicious attacks using mobile agents. Proposed method protects the mobile ad hoc networks through self-organized, fully distributed, and localized mechanisms, in which no secret associations exist between a pair of nodes, and no single node is superior to the others. Proposed mechanism also differs from these secure routing protocols in that it addresses the protection of routing and packet forwarding in a unified framework. There have been

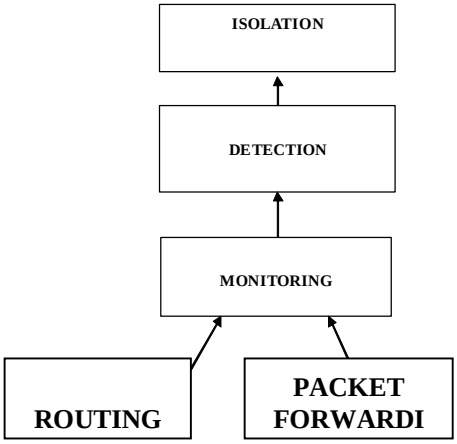
several papers focused on providing self-organized security support in ad hoc networks. However, collaborative consensus mechanism in proposed model provides a complete network-layer security solution that encompasses all three components of protection, detection, and reaction.

In ad hoc networks, multihop packet delivery is achieved through two closely related network-layer operations: ad hoc routing and packet forwarding. As a result, the security solution should encompass the protection of both. The secure ad hoc routing problem has been extensively researched and a number of secure routing protocols have been proposed in the literature, to name a few, Ariadne, SEAD, SRP, ARAN, and SAODV.

All these protocols focus on protecting the correctness of the routing table maintained at each node, while leaving packet forwarding largely unprotected. Moreover, they typically protect the routing messages through various cryptographic primitives, resulting in constant and nontrivial routing overhead in terms of both computation and communication. The companion key management problem is also challenging due to the self-organized nature of ad hoc networks. On the other hand, the secure packet forwarding problem has received relatively little attention. While Watchdog and Pathrater can mitigate the detrimental effects of packet drop in the context of dynamic source routing, its applicability in the distance-vector routing protocols, such as ad hoc on-demand distance vector (AODV) and secure ad hoc on-demand distance vector (SAODV), is not addressed yet. The fundamental problem is that, due to their strong interdependency, routing and packet forwarding should be protected together. To this end, we present a network-layer security solution that protects the control-plane (ad hoc routing) and the data-plane (packet forwarding) operations

in a unified framework. This method does not apply any cryptographic primitives on the routing messages. Instead, it protects routing and packet forwarding through a same reactive approach, in which local neighboring nodes collaboratively sustain each other, monitor each other, and react to occasional attacks in their vicinity.

III. OVERVIEW OF PROPOSED FRAMEWORK



In the proposed design, collaborative monitoring and packet delivery functionality are protected. Each node overhears the wireless channel, and monitors the routing and packet forwarding behavior of its neighbors all the time. The monitoring results at different mobility are cross-validated. A malicious node is convicted when its neighbors reach a consensus, then that particular node is deprived form the network membership and isolated in the network.

In order to improve the network access, each legitimate node carries a valid certificate which is certified, unexpired and not revoked, while any node without valid certificate will be denied of its participation from the network. A legitimate node should always renew the certificate from its neighbors before its current certificate expires. When a malicious node is found, its neighbors collectively revoke its certificate and inform all other nodes in the network. This proposed system has three main components:

1. Monitoring: All nodes within a local neighborhood collaboratively monitor each other.
2. Detection of malicious nodes: All legitimate nodes in a local neighborhood collaboratively renew the certificates for each other. The certificate renewal mechanism ensures legitimate nodes can continue to stay in the network by renewing their certificate from time to time.
3. Isolation: The neighbors of a malicious node, upon consensus, collaboratively revoke its current certificate. This mechanism reacts to occasional attacks launched by malicious nodes by revoking their certificates and alerting the network. This proactively prevents attacker from further disrupting the network, because without a valid certificate it cannot participate in the network.

A. Monitoring

The collaborative monitoring mechanism is used to monitor the routing and packet forwarding operations of each node in a fully decentralized and localized manner. Each node overhears the channel, monitors the behavior of its neighbors, and discovers consistent misbehavior as indications of attacks.

Monitor Routing Behavior

Monitoring is to overhear the channel and *cross-check* the routing messages announced by different nodes. The routing activity of a node is a three-step process:
1) Receiving routing updates from neighboring nodes as inputs to a routing algorithm;
2) Executing the routing algorithm; and
3) Announcing the output of the routing algorithm as its own routing updates.

Monitoring process is used to verify whether the routing algorithm executed by a node follows the protocol specifications. This process is implemented in the context of AODV, in which the routing algorithm is distributed Bellman–Ford algorithm with constraints on sequence number. By overhearing a routing update, an AODV node cannot obtain enough information; reason is that the next hop information is missing in the AODV routing messages. Thus, when a node announces a routing update, its neighbors have no clue about which node is the next hop in the route and, hence, cannot judge on its input to the routing algorithm.

To overcome these disadvantage two modifications to AODV is added. First, we add one field, next_hop, in the RREP packet. Similarly, we add one more field, previous_hop, in the RREQ packet. This way, each node explicitly claims its next hop in a route when it advertises routing updates. Second, each node keeps track of the routing updates previously announced by its neighbors.

Monitor Packet Forwarding Behavior

Each legitimate node also monitors the packet forwarding activity of its neighbors. This is achieved by overhearing the channel and comparing ongoing data transmission with previously recorded routing proposed to work with DSR, in which the sender explicitly lists the route in the data packet header. It cannot be directly applied in the AODV context, because when a node receives a packet, its neighbors do not know to which node it should forward the packet, thus, cannot tell whether it forward the packet in the correct manner. Fortunately, our modification to the AODV protocol, described in the previous section, enables the detection of packet drop, because each node keeps track of the route entries announced by its neighbors, which explicitly lists the next_hop field. A distributed collaborative consensus

mechanism that exploits the collaboration among local neighboring nodes to improve the monitoring performance.

B. Detection of malicious nodes.

Certificate renewal operations are implemented based on an earlier proposal of distributed certification service for mobile ad hoc networks. All the legitimate nodes in the network, carries a certificate which contains the following three fields (owner_id, signing_time, expiration_time). The certificates are protected by the public-key cryptographic primitives. There is a single key pair in the network. The public key is known to all nodes when they join the network, while the secret key is used to sign each certificate. Since the certificate is certified and bound to the owner's unique ID, a malicious node cannot fabricate a certificate or steal the certificate from another legitimate node. This way, the certification service can resist up to k-1 colluding malicious nodes in the network.

Before the current certificate expires, each node solicits its local (typically one-hop or two-hop) neighbors to renew its certificate. The message handshake in this localized certificate renewal process is illustrated in Figure. The node that needs certificate renewal broadcasts a certificate request (TREQ) packet, which contains its current certificate and a timestamp. Each node keeps a certificate revocation list (TRL) based on the certificate revocation mechanism. When a node receives a TREQ packet, the TRL is used to decide whether to serve the request or not. When a node receives a TREQ packet from its neighbor, it extracts the certificate from the packet. It checks whether the certificate has already been revoked by comparing it with the TRL. If the certificate is still valid yet about to expire, it constructs a new certificate with equal to that in the old certificate, equal to the timestamp in the TREQ packet. This is determined by the honesty strategy method. It then signs the newly constructed certificate using its own secret key, encapsulates the partially signed certificate in a TREP (certificate reply) packet, and then unicasts the TREP packet back to the node from which it received the TREQ packet. TREQ packets containing revoked certificates are silently dropped. When the requesting node receives TREP packets from different neighbors, it combines these partially signed certificates into a single certificate signed with secret key.

Honesty strategy is to determine the certificate lifetime which is expiration_time in a certificate. Since the certificate must be renewed once it expires, the legitimate nodes may be penalized by the computation and communication overhead associated with the certificate renewal process. Once a certificate with long lifetime is revoked, it has to be kept by each node in its TRL for a long period of time until it expires, resulting in an increased length of the TRL. Therefore, the certificate lifetime represents a tradeoff between the overhead and the number of states kept at each node.

A proposed method, a novel honesty strategy to determine the certificate lifetime, which can decrease the certificate renewal overhead as time evolves yet keep the TRL length bounded by a constant factor. In this strategy, a newly joined node is issued a certificate with short lifetime. It accumulates its honesty when it remains to behave well in the network, and its subsequent certificate lifetime depends on its honesty at the renewal time. The more honesty one node has, the longer lifetime its certificate has. This way, a legitimate node will have its certificate lifetime steadily increased over time, thus renewing its certificate less and less frequently.

Hence, the expected length of the TRL is also bounded by a constant number. In essence, the honesty strategy takes advantages of the characteristics of node behavior, and rewards well-behaving nodes by decreasing their certificate renewal overhead.

To avoid synchronization of a certificate renewal requests among the nodes, introduction of randomization in the timers is associated .Instead of requesting certificate renewal exactly before, the node randomly picks up a value with uniform distribution over, and broadcasts the TREQ packet at time .

In the collaborative consensus mechanism, local neighboring nodes collaborate with each other to cross-validate the monitoring results at different nodes and reach a consensus. We use "m out of N" strategy as the consensus criteria. That is, a node is considered as an attacker if and only if nodes out of all its neighbors have independently detected its misbehavior. The "m out of N" strategy can significant improve the monitoring performance, which can be quantitatively evaluated by two metrics:

1. Detection probability (correct detection of an attacker) and
2. False alarm probability (false accusation against a legitimate node).

The collaborative consensus mechanism is implemented in a distributed manner. Each node broadcasts a single intrusion detection (SID) packet once it detects the misbehavior of any neighbor. We do not differentiate the SID packets triggered by routing and packet forwarding misbehavior. When a node has received independent SID packets against the same node, it constructs a notification of certificate revocation, signs the notification using its own share of SK, encapsulates the signed notification in a group intrusion detection (GID) packet, and then broadcasts the GID packet. When a node has received GID packets, it constructs a certificate revocation (TREV) packet signed by the SK , using the same polynomial secret sharing primitive as we described in the certificate renewal process.

C. Isolation of malicious nodes

Proposed model revokes a malicious node's certificate in the network. Each node keeps a certificate revocation list (TRL). The certificate revocation process is initiated when a constructed TREV packet is broadcasted. When a node receives a TREV packet, it checks whether the packet is signed by SK, and whether the revoked certificate is already on the TRL. TREV packets that are not signed by or contain certificates on the TRL are silently dropped. Otherwise, it adds the revoked certificate into its own TRL and rebroadcasts the TREV packet. By checking this way every

node will add the revoked certificate into its TRL.

Because only nodes with valid certificates can participate in the network operations, the certificate revocation mechanism ensures that a malicious node is isolated right after it was detected. While the TREV packet is essentially flooded in the network, the associated communication overhead is affordable because there is only one TREV packet per attacker.

Each TRL entry is also associated with a soft-state timer. In order to ensure that a malicious node cannot renew its certificate, a revoked certificate has to be kept in TRL until it expires, after which it can be deleted. This soft state reduces both the storage overhead and the processing overhead when a node checks the validity of the certificates presented by its neighbors.

IV. Simulation results and analysis

In this section, the performance of proposed model is evaluated through extensive simulations. The simulation methodology is started and performance metrics is evaluated. The results show that proposed model is effective in protecting the network layer of ad hoc networks even in a highly mobile and hostile environment.

The proposed model is implemented in the ns-2 simulator. Performance evaluations are based on the simulations of 100 wireless nodes that form an ad hoc network over a rectangular (3000 m 600 m) flat space in 1500 s of simulation time. The physical layer at each networking interface is chosen to approximate the Lucent Wave LAN wireless card. The MAC layer protocol and the routing protocol are 802.11 DCF and modified AODV protocol, respectively. An improved version of "random waypoint" model, which is recently proposed as the mobility model. Set the minimum speed for each node as 2 m/s except for the static network case, and vary the maximum speed to evaluate the impact of node mobility on proposed model performance. The pause time is set to 0 to simulate an ad hoc network in which nodes are constantly roaming. Before the simulation runs, randomly select a certain fraction, ranging from 0% to 40%, of the network population as malicious nodes. Each malicious node picks up a random subset from the pool of possible attacks as its action strategy in the simulations.

The attack pool includes all misbehavior nodes, for example modifying the hop_cnt or seq_number fields in the routing updates (routing misbehavior), dropping or duplicating the data packets, blasting lots of packets (packet forwarding misbehavior). It is possible that a malicious node may select a combination of different misbehavior strategies. In the simulation run, multiple random user datagram protocol (UDP) constant-bit rate (CBR) traffic is sent in the network, each starting at a random time and lasting until the simulation terminates. Vary the number of CBR connections from 10 to 30 and the simulation results all follow the same trend. For simplicity, result is presented where ten CBR traffic is sent. The legitimate nodes participate in the routing and packet forwarding activities in a normal manner, i.e., following all protocol specifications. On the contrary, the malicious nodes attempt to disrupt the network operations according to their preselected strategy.

Collaborative monitoring is done in order to detect the malicious nodes. Collaboratively consensus mechanism is applied in order to detect and revoke the certificate. Monitoring results over the neighbors are cross checked and m malicious nodes are found out. It can be evaluated by detection probability and false alarm probability. An IP SPOOFING attack is introduced, in which legitimate nodes changes its IP address which is detected & isolated by proposed technique.

In the simulations, we are interested in the following metrics:

1. *False accusation ratio*, which is the chance that the proposed method incorrectly convicts and isolates a legitimate node;
2. *Packet delivery ratio*, which is the percentage of packets that are successfully delivered to the receiver nodes; and
3. *Communication overhead*, which is the total number of packets sent by the proposed framework in order to achieve its goal.

In a specific simulation run, due to the constraints of the dynamic network topology, some malicious nodes may not have the chance to realize their preselected attack strategy. For example, a malicious node that plans to drop the data packets can only do so when it resides in an active route. Active malicious nodes are defined, as those that have indeed misbehaved in the network operations, no matter how short the misbehaving time period is. For fairness purpose, the miss detection ratio is obtained by considering only the set of active malicious nodes, instead of all prechosen malicious nodes. The false accusation ratio is obtained in a similar way over the set of active legitimate nodes.

The detection performance of the collaborative monitoring mechanism is evaluated in proposed model in terms of miss detection and false accusation ratios. The collaborative consensus mechanism adopts a "m out of N" strategy, in which is an important parameter that can tradeoff between the miss detection ratio and the false accusation ratio. In these simulations, we fix as 6 because on average two neighboring nodes have about ten common neighbors, and study the impact of mobility and the number of malicious nodes. Figure shows the miss detection ratio as the node mobility speed changes. We can see that this ratio is the highest in a static network, regardless of the number of malicious nodes. In a static network, if a malicious node happens to stay in a sparsely occupied region, its neighbors always have no chance to convict it.

On the contrary, in a mobile network, the mobility increases the chance that other nodes roam into this region or the malicious node itself moves into another densely occupied region. As a result, the malicious node has less chance to escape the monitoring mechanism as there are more legitimate nodes in its neighborhood. When nodes are constantly moving at a high speed, a node can overhear only partial information about previous transmissions of its

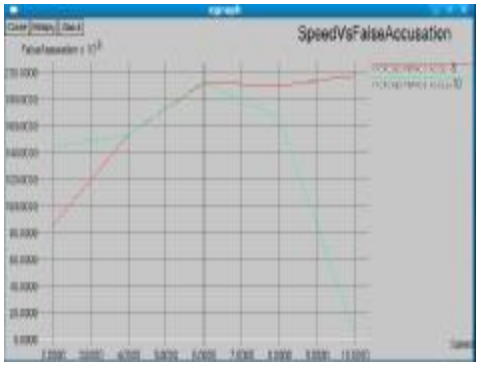
current neighbors. As a result, it is prone to mistakes in cross-checking the incomplete information, and tends to incorrectly accuse its legitimate neighbors. However, even if a single node may have a relatively large chance to do so, the collaborative consensus mechanism can significantly decrease the false accusation ratio by cross-validating the monitoring results from different nodes.

The effectiveness of proposed model can be evaluated from the packet delivery ratio perspective. Figure shows the improvement on the packet delivery ratio in a protected network. In these simulations, 30% of the nodes are set as malicious nodes. We can see from the figure that proposed model increases the packet delivery ratio by a factor up to 150% even if 30% of nodes are malicious. The reason is that after a malicious node starts to launch the attacks, it is detected by its neighbors and its current certificate is then revoked. Therefore, it cannot participate in the network and disrupt the network operations any more. In an ad hoc network without any security protection, the packet delivery ratio can be as low as 30%, even if the network is lightly loaded as in our simulations. On the contrary, the packet delivery functionality is significantly improved in a proposed model network.

Performance analysis Metrics

A. False accusation ratio

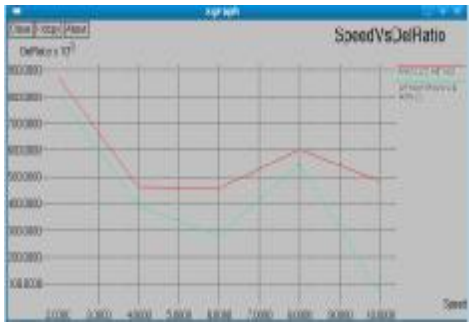
False accusation ratio is the chances that the proposed framework incorrectly convicts and isolates a legitimate node.



This figure illustrates the impact of node mobility in false accusation ratio is presented here. This ratio starts increasing at first as node moves faster. The reason is higher mobility makes node memory less. If a single node have a chance to do so, the collaboratively consensus mechanism can significantly decrease the false accusation ratio by cross-validating the monitoring results from different nodes.

B. Packet delivery ratio

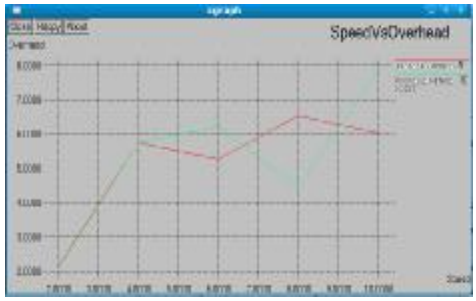
Packet delivery ratio is the percentage of packets that are successfully delivered to the receiver nodes.



From this graph, it is clearly shown that without proposed method the delivery ratio is reduced, but after introducing the collaborative consensus mechanism the delivery ratio is increased. Hence proposed method secures both routing and packet forwarding

C. Communication overhead

Communication overhead is the total number of packets sent by the proposed framework in order to achieve its goal.



V. CONCLUSION

One fundamental challenge for security design in mobile ad hoc networks is the absence of any preexisting infrastructure support. This work explores a novel self-organized approach to securing such networks. To this end, we have presented a proposed model, a network-layer security solution that protects routing and forwarding operations in a unified framework. This model exploits localized collaboration to detect and react to security threats. All nodes in a local neighborhood collaboratively monitor each other and sustain each other, and no single node is superior to the others. The proposed design is self-organized, distributed, and fully localized. Both analysis and simulations results have confirmed the effectiveness and efficiency of the proposed framework in protecting the network layer in mobile ad hoc networks.

REFERENCES

[1] S. Marti, T. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," in Proc. ACM MobiCom, 2000, pp.255–265.
[2] J. Hubaux, L. Buttyan, and S. Capkun, "The quest for security in mobile ad hoc networks," in Proc. ACM MobiHoc, 2001, pp. 146–155.
[3] J. Kong, P. Zerfos, H. Luo, S. Lu, and L. Zhang, "Providing robust and ubiquitous security support for MANET," in Proc. IEEE ICNP, 2001, pp. 251–260.
[4] Y. Hu, A. Perrig, and D. Johnson, "Ariadne: A secure on-demand routing protocol for ad hoc networks," in Proc. ACM MobiCom, 2002, pp. 12–23.

[5] Y. Hu, D. Johnson, and A. Perrig, "SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks," in Proc. IEEE WMCSA, Jun. 2002, pp. 3–13.
[6] P. Papadimitratos and Z. Haas, "Secure routing for mobile ad hoc networks," in Proc. CNDS, 2002, pp. 193–204.
[7] K. Sanzgiri, B. Dahill, B. Levine, C. Shields, and E. Royer, "A secure protocol for ad hoc networks," in Proc. IEEE ICNP, 2002, pp. 78–89.
[8] M. Zapata and N. Asokan, "Securing ad hoc routing protocols," in Proc. ACM WiSe, 2002, pp. 1–10.
[9] S. Capkun, L. Buttyan, and J. Hubaux, "Self-organized public-key management for mobile ad hoc networks," IEEE Trans. Mobile Computing, vol.2, no. 1, pp. 52–64, Jan. 2003.
[10] D. Johnson, D. Maltz, and J. Jetcheva, DSR: The Dynamic Source Routing Protocol for Multi-Hop Wireless Ad Hoc Network, Ad Hoc Networking. Reading, MA: Addison-Wesley, 2001, ch. 5.
[11] C. Perkins and E. Royer, "Ad hoc on-demand distance vector routing,"in Proc. IEEE WMCSA, 1999, pp. 90–100.
[12] J. Broch, D. Maltz, D. Johnson, Y. Hu, and J. Jetcheva, "A performance comparison of multi-hop wireless ad hoc network routing protocols," in Proc. ACM MobiCom, 1998, pp. 85–97.
[13] C. Perkins, E. Royer, and S. Das, "Ad hoc on demand distance vector (AODV) Routin," Internet Draft, draft-ietf-manet-aodv-10.txt, 2002.
[14] S. Das, C. Perkins, and E. Royer, "Performance comparison of two on-demand routing protocols for ad hoc networks," in Proc. IEEE INFOCOM, 2003, pp. 3–12.
[15] Wireless LAN Media Access Control (MAC) and Physical Layer (PHY) Specifications, IEEE Standard, 1999.
[16] S. Buchegger and J-Y.L. Boudec, "Performance analysis of the CONFIDANT protocol", In *Proceedings of the 3rd ACM Symposium on Mobile Ad Hoc Networking and Computing*, pp. 226-236, 2002.
[17] L. Buttyan and J.P. Hubaux, "Stimulating cooperation in self-organizing mobile ad hoc networks", *ACM Journal for Mobile Networks (MONET), Special Issue on Mobile Ad Hoc Networks*, summer 2002.
[18] O. Kachirski and R. Guha, "Effective intrusion detection using multiple sensors in wireless ad hoc networks", In *Proceedings of the 36th Hawaii International Conference on System Sciences*, pp. 57-61, 2003. [19] M.C. Man and V.K. Wei, "A taxonomy for attacks on mobile agents", In Proceedings of the International Conference on Trends in Communications, Vol. 2, pp. 385-388, 2001.]
[19] N.Jaisankar and Brijendra Singh, "Design and Implementation of mobile agents architecture", In National conference on innovations and communication technology (NCIIT-2003) at PSG college of Technology, Coimbatore, March 7-8, 2003.