# An Exchange Framework for Intrusion Alarm Reduction in Mobile Ad-hoc Networks

Shiau-Huey Wang
National Taipei University, Graduate Institute of Information Management, Taipei, Taiwan
Email: angelenew@gmail.com

***Abstract*—Numerous Intrusion Detection Systems (IDSs) have been developed for MANETs; however, comparatively little research focuses on intrusion alarm exchange and validation in Mobile Ad Hoc Networks (MANETs). We provide a secure alarm exchange framework for proactive MANET routing protocols and use Optimized Link State Routing model (OLSR) for the implementation. In our solution, alarms can be aggregated at a group coordinator for advanced alarm verification and reduction. This model can solve two major challenges in MANETs: lack of a centralized authority and dynamic topology caused by mobility. Furthermore, it also provides the foundations for local and global alarm validations. Unnecessary responses to false or forged alarms can be prevented if intrusion alarms are proved to be authentic and accurate. Our model selects the node with the best connectivity as the temporary centralized node for collecting all local alarms. Subsequently, it utilizes majority-voting strategy to detect false alarms. After false alarm reduction, an accurate local alarm is broadcast as a global alarm for notifying the entire network of the attacker existence. This model has the advantages of alarm reduction and low time overhead. The experimental results demonstrate that our solution is scalable and is not influenced by mobility. Extra alarm exchange and verification messages cause low time and message overhead.**

***Index Terms*—MANET, Intrusion Detection, Alarm Validation, Alarm Exchange**

## I. Introduction

Traditional wireless networks have a fixed infrastructure, and all mobile devices use wireless radio to communicate with a base station connected to a wired network. However, a base station does not exist under certain circumstances when a wired infrastructure is not available or not effective; examples include battlefields and disaster areas. These needs are served by Mobile ad hoc networks (MANETs) [1,9]. MANETs are a set of nodes that can communicate with each other without a static base station, a centralized node. These mobile MANET nodes act as both routers and hosts, exchanging routing control messages with each other to establish routing topologies. Routing models in MANET enable mobile nodes to maintain reliable routing tables to reflect the topology change. Because of lack of centralized nodes and dynamic topology, MANETs become extremely vulnerable to attacks. As a result, numerous research efforts have focused on securing MANET models by using cryptography to prevent attackers from participating in the model [12, 13, 14] or by using intrusion detection techniques to further improve the security of MANETs [ 7, 8, 31, 32]. Other research focuses on detecting packet drops [28,29]. However, there are relatively very few efforts dedicated on response systems for MANETs. Therefore, we propose an intrusion alarm exchange framework for MANET. This model is the pioneer which addresses alarm exchange in a fully distributed MANET environment as well as alarm verification to reduce false alarms and catch forged alarms. As a result, unnecessary responses triggered by false or forged alarms can be prevented. We establish an efficient and reliable communication channel among Intrusion Detection agents for MANET. Our alarm exchange model can solve two fundamental issues in MANET: lack of a centralized authority and dynamic topology caused by mobility. Our model can also be utilized to support local and global alarm validation. We apply hierarchy structures to categorize neighboring nodes into groups. MANET nodes in every group will elect the one with the best connectivity as the group coordinator. The coordinator is responsible for collecting all intrusion alarms in its group and uses majority-voting strategies to perform local alarm verification to discover false positives.

The experimental results demonstrate our proposed solution is scalable and not influenced by mobility. Scalability is achieved because local alarm exchange happens within groups. Adaptability to the mobile environments is guaranteed because a group coordinator has the best connectivity such that it still has connected neighbors as next hops while some others move away. In this work, we use Optimized Link State Routing model (OLSR) as the target for implementation, and the experimental results show short response delay and high mobility resilience.

The remainder of this paper is organized as follows: Section 2 discusses the problem statement. Section 3 presents our alarm exchange and validation model. Section 4 evaluates the performance; Section 5 concludes and explores future work.

## II. Related Work

Numerous research efforts have focused on securing MANET protocols by using cryptography to prevent attackers from participating in the protocol [6,13] or by


doi:10.4304/jcp.8.7.1648-1655

using intrusion detection techniques to further improve the security of MANETs [2, 3, 4, 15]. However, there are very few efforts dedicated on response systems for MANETs.

Automated intrusion response has been studied for *wired networks*. Most research focuses on how to select the best response action to ensure that the response action will improve the security posture and availability of the system. A study by Toth et al. [16] proposes a promising model for automated response. They construct dependency trees that model configuration of the network and give an outline of a cost model for estimating the effect of a response. Balepin [17] followed the idea and developed a cost model to reason automated response at the host level, and this cost model can select an optimal response even in the presence of uncertainty. These approaches, designed for wired networks or hosts, which usually assume fixed configuration and topology, cannot be applied directly to MANETs.

The pioneer research with regard to automated response for MANETs [30] uses topology dependency to evaluate damage and response cost. IDS will take different responses depends on the attacker's topology criticality. Research about alarm processing emphasizes on the development of alarm confidence metrics as an intrusion response reference [19, 20]. Alternatively, correlating alarms to sort alarm events and reduce alarm numbers are also studied [25, 26, 27, 33]. In wired networks, alarms are either flooded to the entire network or sent to a designated server. Due to limited bandwidth and dynamic network topology, new mechanism is desirable for propagating alarms in MANETs. Other works develop signaling systems [10,34] to automatically decide which alarm is urgent for notification without human intervention. Finally, alarm reduction [11,18] is also of interest to researchers. Nevertheless, these approaches, designed for wired networks or mobile networks with base stations, cannot be directly applied to MANETs.

In current intrusion detection and authentication works for MANETs, each node has its own security agent, detecting attacks and reporting intrusion alarms independently. In these works, nodes do not correlate their alarms, and very few alarm correlation and validation works were found in the literature for MANETs. Even in intrusion detection works of MANETs, they simply proposed detection mechanism without addressing how to exchange information among distributed mobile nodes. Our work is the first to propose a general exchange framework for alarm reduction of MANETs, which address exchanging alarms in a fully distributed MANET environment as well as proposing a framework for future alarm validation .

## III. Problem Statement

IDSs can be deployed on gateways, switches, or a selected node in wired networks because of the static topology and trustworthy central points. In order to detect routing attacks, aggregating all routing information on a trustworthy point to some degree is necessary because sufficient information and evidence is required for detection and response purposes. However, MANET possess decentralized communication architecture and mobility nature, hence most IDSs developed for MANETs [2, 3, 4, 5, 6] is fully distributed rather than using a central monitoring point. In the distributed IDS (Figure 1), each node has an IDS installed and monitors its 1-hop neighbors. In other words, neighboring nodes monitors the routing activities and routing messages mutually. If any anomaly is detected, alarms against some suspicious neighbor are raised. Our goal is to develop a real-time alarm exchange and validation model to cooperate with MANET IDS whose architecture is as described in figure 1.

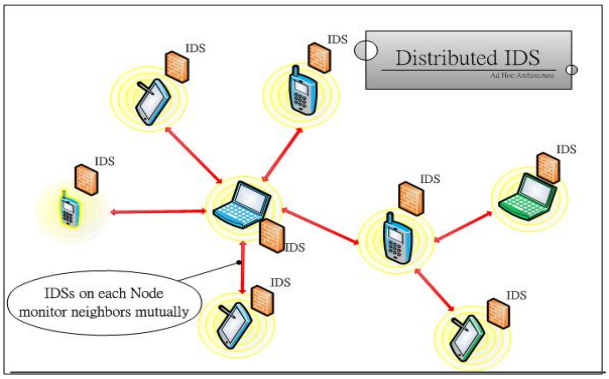



Figure 1. Distributed Architecture for Cooperative Detection Systems

Our model provides reliable alarm exchanges among distributed IDS agents and offers the ease of performing local and global alarm validation. To develop this alarm exchange and validation model, the main challenges encountered are discussed in the following.

### A. Alarm Exchange

As described in figure 1, IDS agents monitor neighbors mutually. Once an attacker is detected, there should be multiple alarms raised since this attacker might have not only one neighboring nodes. Therefore, exchanging alarms in the same group to validate alarms cooperatively is beneficial to discover false positives or forged alarms. However, as discussed, fully distributed MANET has no centralized point for aggregating all alarms. Furthermore, the mobility even increases the difficulty of exchanging alarms among IDS agents reliably since nodes might leave or join some locality. Therefore, how to establish a reliable communication channel among distributed IDS agents in the same group monitoring the same node is critical. To develop a secure communication model, the node monitored by all IDS agents should be avoided being on exchanging paths. Besides, the IDS agents in the same group should be kept well connected, even as network topology changes. However, very few works addressed alarm exchange issues in MANETs.

### B. Alarm Reduction and Validation

This model should provide basic mechanism to reduce false positives and discover forged alarms among neighbors locally. Furthermore, our exchange model can

be a basis for developing global alarm verification in the future. Mobile nodes in MANET can roam freely in the networks. Even if attacker has been detected in some locality, it can move to another position and launch repeated attacks to unwitting nodes in another locality. In order to prevent this recurring attack, it is necessary to propagate local alarms as global alarms to notify the entire network of attackers' identities. However, if a node N receives a global alarm, this global alarm still might be a forged alarm which is fabricated by an attacker to maliciously accuse a benign node. In this situation, node N does not have any related information to validate the forged alarm globally. Our work focuses on the time overhead of local alarm reduction and the global alarm transmission.

## IV. Alarm Exchange and Reduction Model

Our proposed solution is to categorize neighboring nodes as different groups. Each group will elect their own group coordinator as the temporary central node to aggregate all alarms within that group. In the following, "group" definition is given.

### A. Group Architecture

***Nodes of the same "GROUP G" are nodes monitoring the same node.***

As shown in figure 2, many groups exist in our alarm exchange and validation model. In the model, 1-hop neighbors monitors each other and perform distributed monitoring. Nodes that monitor the same node are viewed as being in the same group. In other words, any node's 1-hop neighbors form a collaborative monitoring group. In each group, the physically central node is the node being monitored. Apparently, this central node cannot be the centralized coordinator responsible for collecting alarms for validation. Therefore, an algorithm to find another centralized node as **group coordinators** for advanced alarm processing must be developed.

In the design of this alarm exchange and validation model, we define **Local alarm** as the alarms being raised within a group. Local alarms are aggregated at the group coordinator to validate alarm accuracy for alarm reduction. Local alarm is named in contrast to **Global alarm**, a broadcast alarm by Coordinator to prevent a mobile attacker from performing recurring attacks. We leave Global Alarm Verification as the future work. In our work, we only simulate the time required for a remote node to receive a global alarm. The main idea of our solution model is to elect the most appropriate candidate as the group coordinator. This temporary coordinator collects all related local alarms for verification. After performing verification, false alarms and forged alarms can be discovered and reduced. Subsequently, a global alarm is broadcast to the entire network.

### B. Alarm Attack Model

Table I describes the two attack events in our attack model regarding alarms only. Our alarm exchange and validation model can solve Type 1 and Type 2 alarm attacks.

TABLE I.
Alarm Attack Model

| Attack Types | Attack Description |
|---|---|
| Type 1: Forge initiated alarms | Attackers can initiate forged local alarms or global alarms. |
| Type 2: Forge forwarded alarms & node identity | Attackers can disrupt the integrity of forwarded local or global alarms by modifying the contents of alarms passing through it. Furthermore, the attacker can also fabricate a non-existing alarm by pretending that he is forwarding it. |
| Type 3: Drop forwarded alarms | A selfish node may drop alarms routing through it. If a selfish node drops a unicast local alarm or a broadcast global alarm, the dropped alarms may still reach the nodes supposed to be reached because of the flooding nature. Besides, several reputation-based works have been proposed to prevent a node from dropping packets intentionally [28, 29]. |

### C. Alarm Exchange

Figure 3 illustrates our proposed model for alarm exchange and validation. Once a node receives a local alarm, it acquires the member list of group G, and then elect a node as the group coordinator C. After group coordinator C is determined, each node unicasts its own local alarm to C; then local alarm validation is performed at C. Once passing local alarm validation, a global alarm will be prepared to be broadcast to the entire network. Subsequently, remote nodes perform global alarm validation upon the receipt of this global alarm.

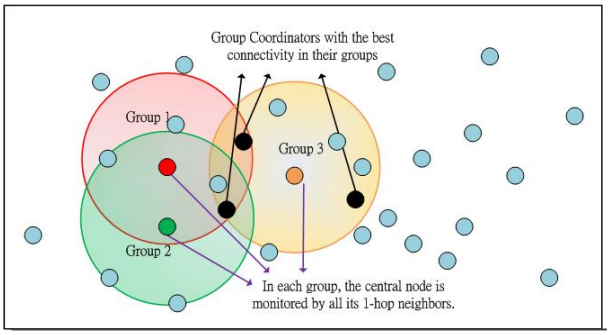



Figure 2. Groups in Alarm Exchange and Validation

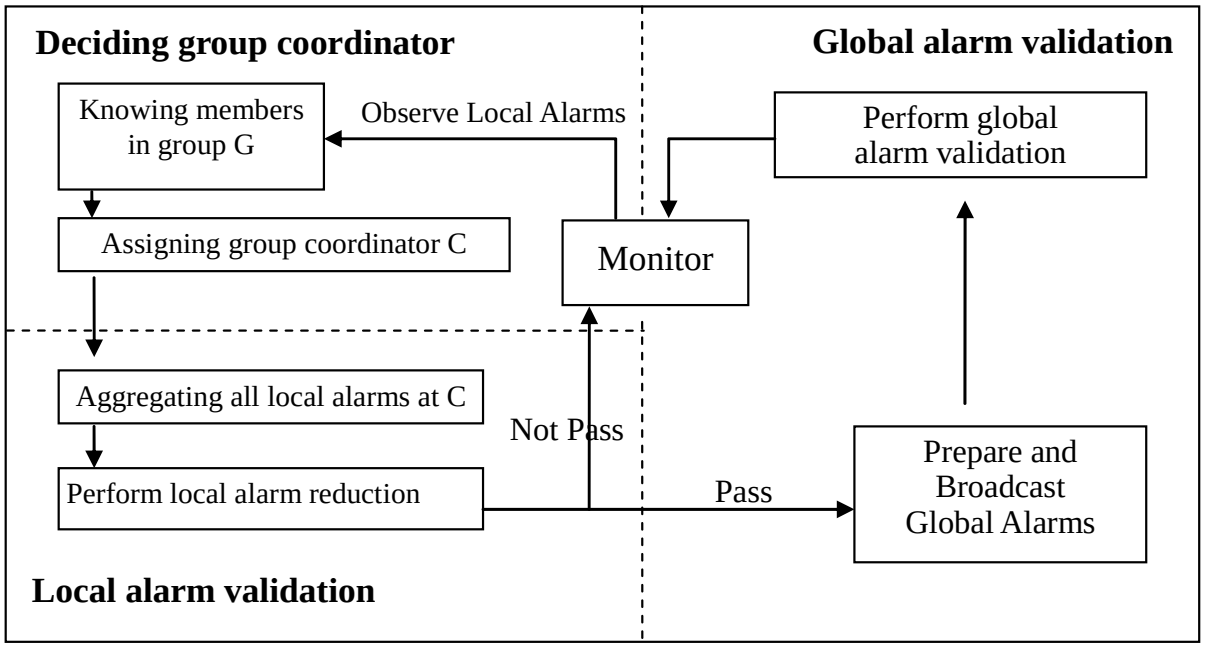



Figure 3. Flow Chart of Alarm Exchange and Validation

The detailed mechanism of alarm validation will be the future work of this paper.

**Obtaining the Member List of Group G**: The IDS architecture our alarm validation model cooperates with is presented in Figure 1, where each node is monitored by all its 1-hop neighbors. Therefore, the distance of the nodes of the same group G is within 2-hops. For a node N to know the member list of group G it belongs to, node N must know 1-hop neighbors of its own 1-hop neighbors, and then it will have the complete knowledge of its neighbors within 2-hops.

**Electing the coordinator C**: After the member list of Group G is obtained, determining how to elect a proper node as the group coordinator C is crucial. The goal of assigning C is to elect a node with better connectivity to other nodes within the same group. In our design, we assign the node with ***the largest number of 1-hop neighbors*** as coordinator C. If there are multiple nodes with equivalent number of neighbors, the node with the smallest MAC address is selected. The reason to choose the node with the largest number of 1-hop neighbors as group coordinator is because this maintains ***better connectivity*** in a mobile environment. The experimental results also show that mobility has little influence on our design.

Figure 1. **Aggregating Local Alarms**: After Coordinator is determined, each node unicasts its own local alarm to group Coordinator C. During the process of alarm aggregation at Coordinator C, nodes in each group G might be disconnected since they need to route to each other without hopping through the attacker, their originally shared 1-hop neighbor. Once any partition occurs in group G, subgroups need to elect their new group coordinators iteratively.

**Handling Mobility**: Mobility is a major issue while aggregating ALL alarms at the coordinator C. Even if we select the node with the best connectivity as the coordinator, mobility still causes at least some unicast paths to the coordinator to be broken. This broken link might result in alarm loss such that the coordinator cannot collect all the alarms within its group. In order to solve this alarm loss problem, we add a **timeout** mechanism to ensure reliable alarm aggregation. In Figure 4, if the coordinator does not receive particular local alarm in a reasonable period of time, it checks whether this lost alarm affect the validation result or not. For example, lacking one alarm has no influence on the decision of majority voting. In such a case, coordinator will proceed to broadcast global alarms or discard local alarms depending on the validation result; otherwise, the coordinator will broadcast an **Alarm Request message (AREQ)** to request the lost alarm when timeout is reached. Once the lost alarm's owner receives an AREQ, it will re-transmit the lost local alarm to the coordinator again. This mechanism can solve message loss problem in a mobile environment. Timeout of AREQ is **1 second**. Furthermore, the timeout for collecting local alarms is **3 seconds**. If the coordinator still does not receive all local alarms within 3 seconds, the coordinator will perform local validation immediately and then broadcast the global alarm. This timeout mechanism helps resolve the situation where the coordinator cannot receive all local alarms because of broken links caused by node mobility.

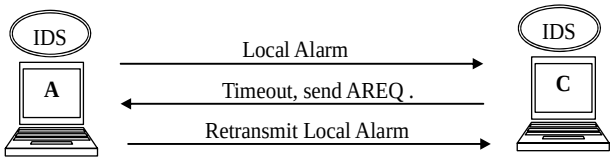



Figure 4. Alarm Request message (AREQ).

### *D. Local Alarm Reduction and Global Alarm Transmission*

Experimental data shows that most false positives occur when only one of the neighbors of the suspicious node raises a false alarm. In other words, if the number of neighbors of the suspicious node who raise the alarm is no larger than those who do not raise the alarm, the alarm should be considered a false positive or forged alarm. This is because many routing protocols of MANETs use broadcast routing messages. If an attacker broadcasts a corrupted routing message, all distributed IDSs should hear it. Since each detector hears the same routing messages and has the same security rules applied, all detectors should ideally have the same detection decision against the monitored node. Besides OLSR, this Majority-Voting strategy can also be applied to IDSs for ARAN [23], AODV IDSs [24], and other protocols as well. After a local alarm is well verified, coordinator C broadcast it to the entire network as a global alarm. Our simulation will calculate how much time overhead from a local alarm is raised to a global alarm is received by a remote node.

In order to protect the integrity and authenticity of both local and global alarms, each group node can use DSA [22] to digitally sign its own local alarm and then send it to the coordinator C. This can prevent local alarms from being modified during aggregation process. It also can prevent a malicious node from impersonating others to send a fake local alarm that disturbs the local alarm reduction. The coordinator will broadcast a global alarm only when the integrity and authenticity of all local alarms are proven and the majority agrees with the attacker existence. Once a remote node receives this global alarm, it can use the corresponding public keys to respectively verify all signatures of each group node joining majority voting process. If all digital signatures are correct, then this global alarm passes the validation. Since a global alarm is broadcast only when the signatures of all RAs are correct and pass local alarm validation, the sender of a global alarm must be malicious if the global alarm cannot pass validation globally. Our work provides a well-designed alarm exchange framework for performing advanced local and global alarm validation. However, at this point, we only focus on evaluating the time overhead and mobility resilience of our proposed solution.

## V. Alarm Exchange and Reduction Model

Optimized link state routing protocol (OLSR) is used in our experiment. We implement the mechanisms of selecting group coordinator, local alarm aggregation and lost alarm request under different network scales and different mobility degrees.

### *A. Experimental Protocol OLSR*

OLSR is a link-state, proactive routing model in MANET. In OLSR, periodical Hello and Topology Control (TC) messages are two main routing messages used to establish a complete network topology among nodes. Furthermore, OLSR utilizes MPRs, a minimum subset of 1-hop neighbors connecting all 2-hop neighbors, to reduce overhead of flooding messages. With these design characteristics, OLSR provides a more robust and complete routing topology compared with other reactive models in MANETs while maintaining reasonable routing message overhead in a resource-precious MANET.

In OLSR, the computation of routing tables depends on three critical fields in Hello and TC messages: 1-hop neighbors and MPRs in Hello message as well as MPR selectors in TC messages. A node can send three types of basic OLSR messages: Hello, initiated TC, and forward TC messages.

### *B. Experimental Environment and Matrices*

*GloMoSim* is our experiment platform and is a simple, effective, and scalable simulation environment for MANETs. The simulation is based on 802.11 and Ground Reflection (Two-Ray) Model, which has both a direct path and a ground reflected propagation path between the transmitter and receiver. Given the default signal propagation parameters in GloMoSim, the radio range is about 380 meters. Each node in our simulation moves according to the random waypoint model [21]: each node randomly chooses an arbitrary destination, and it moves toward the chosen destination with a speed of up to 20 m/s (45 miles/hr). Once the node reaches the destination, it stays in that location for a pre-determined pause time. The node then randomly chooses another destination and the procedure is repeated.

In our simulation, three messages are designed and described in the following:

**Local Alarm**: In table II, a local alarm message has 12 bytes: 4 bytes for its own (sender) IP address, 1 byte for message type, 1 byte for detection decision, 1 byte of reachable RAs in group G, 1 byte for indicating the response session, 4 bytes for the IP address of the suspicious attacker. RAs of the same group G might be disconnected since they route to each other without hopping through the monitored node, their originally shared 1-hop neighbor. Once any partition occurs in group G, subgroups needs to elect their new temporary coordinators, respectively. Therefore, the numbers of reachable RAs helps track the reliability of our framework, much like reflecting the connectivity of response agent does.

TABLE II.
MESSAGE CONTENT OF LOCAL ALARM

| Response Agent Address (RA, Alarm sender) | | | |
|---|---|---|---|
| Type | Decision | num of reachable RAs | Response session num |
| Monitored Node's Address | | | |

**Global Alarm**: In table III, A global alarm carries the response agent list and it has (12+4N) bytes: 4 bytes for the coordinator address, 1 byte for message type, 1 byte

of reachable RAs in group G, 1 byte for non-reachable RAs in group G, 1 byte for future usage, 4 bytes for attacker address, 4*(N-1) bytes for the rest RAs' addresses.

TABLE III.
MESSAGE CONTENT OF GLOBAL ALARM

| Coordinator Address | | | |
|---|---|---|---|
| Type | num of RAs | num of disconnected RAs | Reserve |
| Attacker's Address | | | |
| RA address(es) | | | |

**Alarm Request**: In table IV, an Alarm Request message (AREQ) has 12 bytes: 4 bytes for the coordinator's (sender) IP address, 1 byte for message type, 1 byte for the number of request tries, 2 reserved bytes, 4 bytes for the IP address of the suspicious attacker. AREQ is sent to the RA whose local alarm is not received in time. Timeout of AREQ is 1 second. Therefore, the coordinator will send AREQ to nodes whose local alarms are not received each second. Furthermore, the timeout for collecting local alarms is 3 seconds. If the coordinator still does not receive all local alarms within 3 seconds, the coordinator will perform local validation immediately and then broadcast the global alarm. This timeout mechanism helps resolve the situation where the coordinator cannot receive all local alarms because of broken links caused by node mobility.

TABLE IV.
MESSAGE CONTENT OF ALARM REQUEST

| Coordinator Address | | |
|---|---|---|
| Type | Number of Tries | Reserve |
| Monitored Node's Address | | |

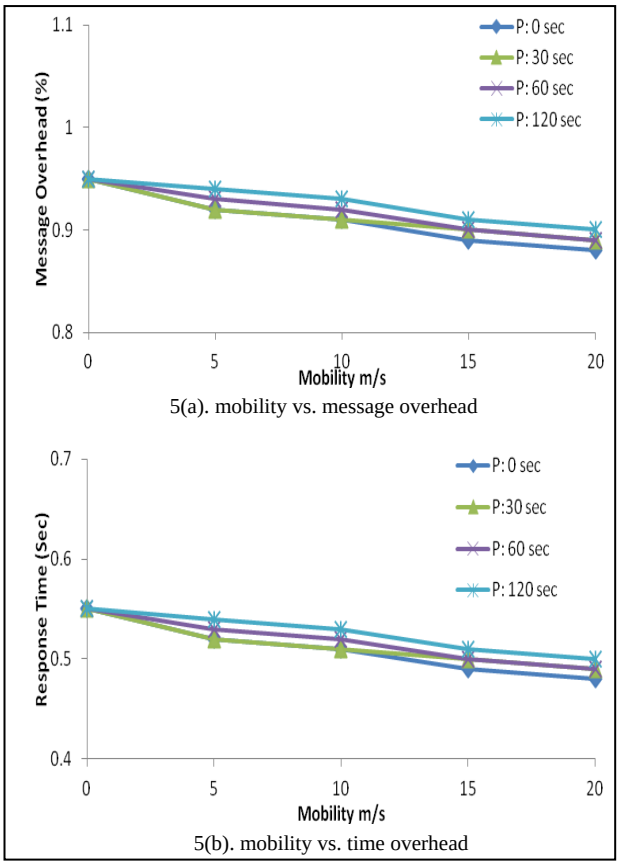
We computed two matrices for each simulation run. The first matrix is **Message overhead**, used to Measure the byte overhead that our proposed model brings to the entire network. The formula of message overhead is:

$$\frac{\text{local alarms} + \text{AREQ} + \text{retransmitted local alarms} + \text{global alarms}}{\text{total network routing messages}}$$

The second matrix is **Response time overhead**, used to measure the time overhead of collecting and validating local alarms at the coordinator in our model. The time from the point a response agent raises an alarm to the point that a global alarm is broadcast to the entire network.

About 200 testing cases were run using different sizes of network topologies and with different degrees of mobility. Network topologies consist of six types of topologies: 25 and 50 nodes in 1km x 1km, 75 and 100 nodes in 1.5km x 1.5km, 125 and 150nodes in 2km x 2km. We repeat each testing case in 5 different pseudo-random seeds. Mobility is tested with random speeds: up to 5, 10, 15, and 20 meters/second and pause times of 0, 10, 20, 30, 40, 50, 60, and 120 seconds. We discuss the two metrics in three kinds of testing conditions: mobility, scalability, and number of RAs.

### C. Experimental Results




5(a). mobility vs. message overhead

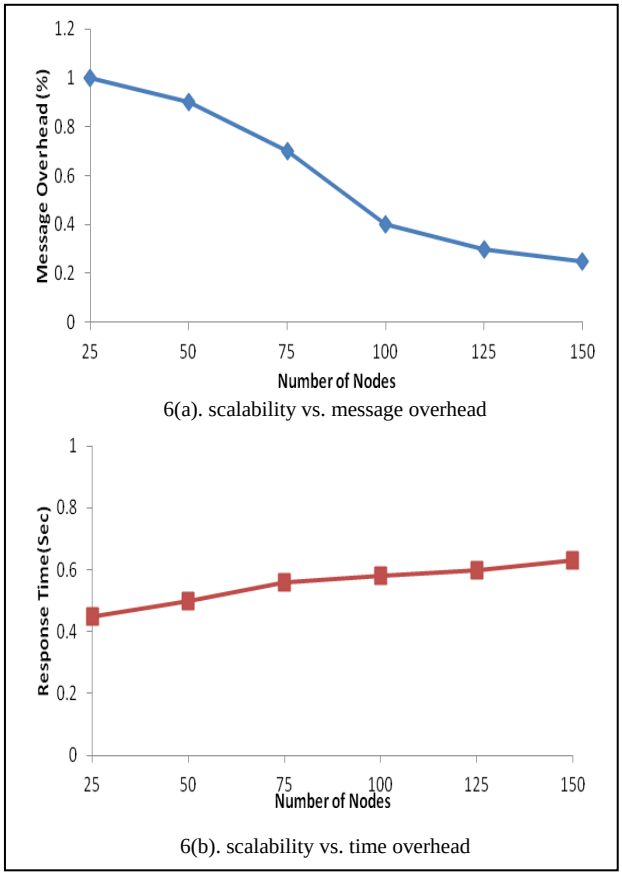
5(b). mobility vs. time overhead

Figure 5. Message & Time Overhead influenced by Mobility

***Mobility*** Figure 5 shows that message overhead and response time overhead are almost the same with different speeds and pause times. Our model is proved to be reliable under different degrees of mobility. This is because we choose the node with the best connectivity as the group coordinator and such that the connectivity between the coordinator and other group nodes is not easily broken as the nodes are moving.

***Scalability*** Shown in figure 6, message overhead decreases as the number of nodes increase because the number of routing message increases a lot (especially forwarded TC messages due to the large network topology) but the number of response messages remains the same. Response time also indicates that our model is scalable, in the sense that the response time does not increase as the size of network increases. Furthermore, we observe that the response time is changed by the group size.

***Group Size*** Group size means the number of nodes in a group. In figure 7, the number of RAs (group nodes) increases as the network becomes denser. However, as

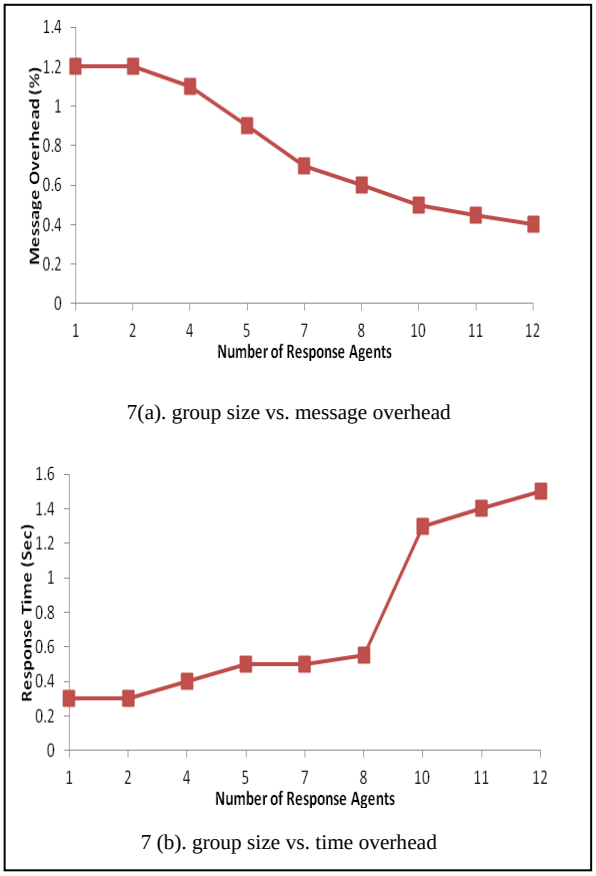



6(a). scalability vs. message overhead

6(b). scalability vs. time overhead

Figure 6.

Message & Time Overhead influenced by Scalability




7(a). group size vs. message overhead

7 (b). group size vs. time overhead

Figure 7.

Message and Time Overhead influenced by Group Size

the network becomes denser, routing messages increase much faster than alarm messages. Consequently, as group size becomes larger, message overhead decreases. On the other hand, while group size becomes larger, response time increases because the coordinator may need more time to aggregate local alarms from group nodes. This shows that our mechanism is very scalable.

## VI. Conclusion and Future Work

We have developed an efficient and scalable model for alarm exchange and validation in MANETs. It not only provides a means of communication for alarm validation, but also allows nodes to exchange information with each other using low message overhead and short time delay. This model can solve two major challenges of MANETS: lack of a centralized node and mobility. In the future, we plan to work on implementing DSA related cryptography on our framework. Besides, we also target at applying our framework to reactive MANET routing protocols, such as AODV in which neighbor information within 2 hops is not as complete as proactive protocols. Subsequently, we will use our proposed model as the communication protocol to perform cooperative decision processes among all nodes to perform cost-sensitive responses determined by response expert system.

## References

[1] P. N. Raj, and P. B. Swadas, "DPRAODV: A Dynamic Learning System Against Blackhole Attack In AODV Based MANET", *International Journal of Computer Science Issues*, IJCSI, 2009.

[2] C.Y. Tseng, S.H. Wang, C. Ko, K. Levitt, "DEMEM: Distributed Evidence-Driven Message Exchange Intrusion Detection Model For MANET", *Proceeding of the 8th International Symposium, RAID 2006, Recent Advances in Intrusion Detection*, Hamburg, Germany, September 20 - 22, 2006

[3] C. Tseng, T. Song, P. Balasubramanyam, C. Ko, Karl Levitt, "A Specification-based Intrusion Detection Model for OLSR", *Proceeding of the 8th International Symposium, RAID 2005, Recent Advances in Intrusion Detection*, Seattle, WA, September 7-9, 2005.

[4] C. Tseng, P. Balasubramanyam, C. Ko, R. Limprasittiporn, Jeff Rowe, and Karl Levitt, "A Specification-Based Intrusion Detection System For AODV", *In Proceedings of the ACM Workshop on Security in Ad Hoc and Sensor Networks* (SASN'03), October 2003.

[5] B. Sun, X. Jin, K. Wu, Y. Xiao. "Integration of Secure In-Network Aggregation and System Monitoring for Wireless Sensor Networks", *IEEE International Conference on Communications, 2007. ICC '07.*

[6] K. Sanzgiri, B. Dahill, B.N. Levine, C. Shields, and E.M. Belding-Royer, "A secure routing protocol for ad hoc networks", *in Proceeding of the Tenth IEEE International Conference on Network Protocols*, 2002.

[7] Y. Zhang and W. Lee. "Intrusion Detection in Wireless Ad-Hoc Networks", I*n Proceedings of The Sixth International Conference on Mobile Computing and Networking*, Boston, MA, August 2000.
[8] R. RameshKumar , A. Damodaram, "ODASARA: A Novel on Demand Ant BasedSecurity Alert Routing Algorithm for MANET in Grid Environment", *International Journal of Computer Science and Network Security*, VOL.10 No.4, April 2010.
[9] T. Clausen, P. Jacquet, "Optimized link state routing model (OLSR)". IETF RFC3626.
[10] N. J. Gerner, T. P. Schmit, "System and Method for Adjusting a Security Level and Signaling Alarms in Controlled Areas", US Patent 8242905, 2010.
[11] H. Om, A. Kundu ,"A hybrid system for reducing the false alarm rate of anomaly intrusion detection system", *1st International Conference on Recent Advances in Information Technology* (RAIT), 2012.
[12] S. Yi, P. Naldurg, and R. Kravets, "Security-aware routing model for wireless ad hoc networks," *in Proceeding of ACM MobiHoc* 2001, Oct 2001.
[13] L. Zhou and Z. J. Haas, "Securing ad hoc networks," *IEEE Network*, vol. 13, no. 6, pp. 24-30, 1999.
[14] K. Sanzgiri, B. Dahill, B.N. Levine, C. Shields, and E.M.Belding-Royer, "A secure routing model for ad hoc networks", in Proceeding of the Tenth *IEEE International Conference on Network Models*, 2002.
[15] R. Rao and G. Kesidis, "Detection of malicious packet dropping using statistically regular traffic patterns in multihop wireless networks that are not bandwidth limited", *Brazilian Journal of Telecommunications*, 2003.
[16] T. Toth, C. Kruegel. "Evaluating the impact of automated intrusion response mechanisms", *18th Annual Computer Security Applications Conference*, Las Vegas, Nevada, December 9-13, 2002.
[17] I. Balepin, S. Maltsev, J. Rowe, K. Levitt, "Using Specification-Based Intrusion Detection for Automated Response," Proceeding of the 6th International Symposium, RecentAdvances in Intrusion Detection, Pittsburgh, PA, September 8-10, 2003.
[18] C. H. Rowland, "method and system for reducing the false alarm rate of network intrusion systems", US Patent 7805762 , 2010.
[19] A. Porras and P.G. Neumann, "EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances", *Proceedings of the National Information Systems Security Conference*, October 1997.
[20] G. B. White, E.A. Fisch, and U.W. Pooch, "Cooperating Security Managers: A Peer-Based Intrusion Detection System". *IEEE Network*, pp. 20--23, vol. 10, num. 1, 1996.
[21] T. Camp, J. Boleng, V. Davies. "A Survey of Mobility Models for Ad Hoc Network Research,", *Wireless Communications & Mobile Computing (WCMC)*: Special issue on Mobile Ad Hoc Networking: Research, Trends and Applications, 2002.
[22] "Digital Signature Standard", FIPS 186.
[23] K. Sanzgiri, B. Dahill, B. N. Levine, E. Belding-Royer, and C. Shields, "A Secure Routing model for Adhoc Networks", *Proceedings of International Conference on Network Models*, 2002.
[24] Y. Huang and W. Lee, "Attack Analysis and Detection for Ad Hoc Routing Models", *Proceedings of International Symposium Recent Advances in Intrusion Detection* (RAID) 2004.
[25] H. Debar, A. Wespi. "Aggregation and Correlation of Intrusion-Detection Alerts ", *Proceeding of the 4th International Symposium, Recent Advances in Intrusion Detection.*, 2001.
[26] F. Cuppens, A. Miege, "Alert correlation in a cooperative intrusion detection model", *Proceedings of 2002 IEEE Symposium on Security and Privacy*.
[27] K. Julisch, M. Dacier, "Mining intrusion detection alarms for actionable knowledge", *Proceedings of the eighth ACM SIGKDD international conference on Knowledge discovery and data mining*, 2002.
[28] F. Anjum and R. R. Talpade, "LiPad: Lightweight Packet Drop Detection for Ad Hoc Networks," *In Proceedings of the 2004 IEEE 60th Vehicular Technology Conference*, Los Angeles, September 2004.
[29] Y. Rebahi, V. Mujica, C. Simons, D. Sisalem, "SAFE: Securing pAcket Forwarding in ad hoc networks", 5*th Workshop on Applications and Services in Wireless Networks*, June/July 2005, Paris, France.
[30] S. Wang, C.Y. Tseng, K. N. Levitt, M. Bishop: "Cost-Sensitive Intrusion Responses for Mobile Ad Hoc Networks", *International Symposium on Recent Advances in Intrusion Detection (RAID)*, Gold Goast, Australia, September 5-7, Lecture Notes in Computer Science 4637, p127-145, Springer 2007.
[31] W. Wang, H. Wang, B. Wang, Y. Wang, J. Wang. "Energy-aware and self-adaptive anomaly detection scheme based on network tomography in mobile ad hoc networks", *Information Sciences*, Volume 220, Pages 580 – 602, 20 January 2013.
[32] J. Choi , K. Shim , S. Lee ; K. Wu ,"Handling Selfishness in Replica Allocation over a Mobile Ad Hoc Network", *IEEE Transaction on Mobile Computing*, Volume11, Issue 2, Pages 278 – 191, Feb, 2012.
[33] H. Chao, C. Hsiao, W. Su, C. Hsu, C. Wu. "Modified adaptive resonance theory for alarm correlation based on distance hierarchy in mobile networks.", *Network Operations and Management Symposium (APNOMS)*, 2011 13th Asia-Pacific.
[34] J. He , Z. Fang, Z. Lu, H. Sun, and W. Xu, "Vector-Based Distributed Mobile Communication Core-Network Intrusion Alarm System", *Future Computing, Communication, Control and Management, Lecture Notes in Electrical Engineering*, Volume 144, 2012, pp 33-40.

**Shiau-Huey Wang** received the Ph.D. degree in computer science from University of California, Davis, CA, in 2008. She is currently an Assistant Professor with the Graduate Institute of Information Management, National Taipei University, Taipei, Taiwan. Before joining NTPU, she worked as software engineer at IBM research in San Jose CA, USA, and Institute for Information Industry (III) in Taiwan, and Assistant Professor with the Department of Information Management, Chung Yuan Christian University (CYCU) in Taiwan. Her current research interests include wireless ad hoc networks, social network marketing, data mining, and network security.