Securing Mobile Ad-Hoc Networks

CNT 6517 Mobile Computing Spring 2016

Nicholas Petty
Computer Science Graduate Student
Florida Atlantic University
Boca Raton, United States

Maciej Medyk
Computer Science Graduate Student
Florida Atlantic University
Boca Raton, United States

***Abstract*— Technological advances in the last two decades have made personal computing more mobile than ever, while increasing the depth and breadth of connectivity. These trends are creating new uses for networks that support device to device communication, rather than the long-established client to server model. Component presence is not dependable in such a network, and flexible infrastructure is required for success. This is the mobile ad hoc network, or MANET: a group of connected computers that may or may not be stationary, can come and go from the network at any time, and are deployed for a specific purpose. As the popularity and utility of MANETs grows, the problems they present must be addressed. One of the most critical issues these networks face is security: since sharing is a cornerstone of implementation, it is vulnerable to infiltration. This paper examines various security protocols, security goals, threats, and challenges in securing a mobile ad hoc network. Specifically the topics of MANET attacks and defenses, both theoretical and applied, are covered. The end of result is a comprehensive view of existing security issues, with the ability to propose solutions based on currently available protocols.**

I. INTRODUCTION

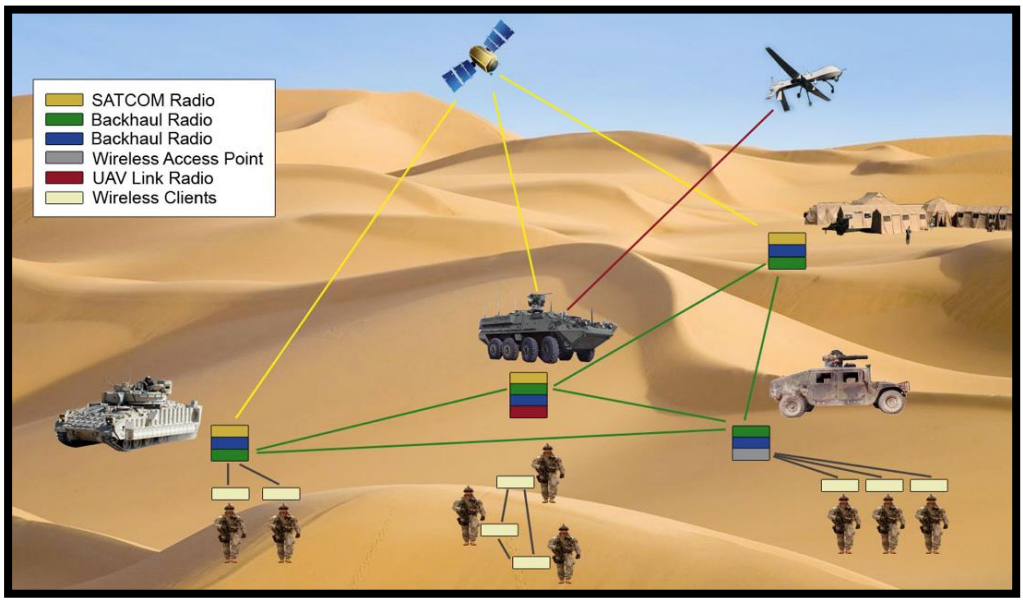
Modern computing is networked computing. The Internet has ushered in a new age of communication, built on the networking of millions of computers. Following this lead, the Internet of Things is poised to revolutionize task automation and data collection. The cornerstone of this technology is a system for building networks from heterogeneous, mobile, battery-powered, wireless devices – the Mobile Ad-hoc Network. While wired computer networks have been tremendously successful, wireless networks have only begun to surge in popularity in recent years. This is due to the convergence of reduced hardware size, increased networking power, longer-lasting batteries, and consumer demand for electronic products (History and Evolution of Cell Phones). Many of the obstacles that mobile networks must overcome are due to hardware limitations, but the issue of security in such a network is something that must be addressed at multiple levels. To evaluate the effectiveness of a security system in a mobile ad-hoc network, or MANET, this paper will introduce what a MANET is and the general networking protocol one employs, then discuss the vulnerabilities resulting from this protocol. After that, currently available security methods will be covered and an actual implementation of a mobile ad-hoc networking will be examined. The paper will conclude with an estimation of value for existing security techniques and recommendations on the future of mobile network security.

II. MANET DESCRIPTION

A mobile ad-hoc network is a group of two or more computing devices that communicate wirelessly to achieve some specific purpose (Mahgoub). The physical components of this network may be general-use computers or functionally limited devices, like sensors. These are the nodes of the network, and they work together in a cooperative system. This system also gives its members equal power and does not rely on a central authority to regulate behavior (Stojmenović). Because they are mobile, nodes do not have a reliable power source and must be conservative with resource expenditure. The network is connected through a

wireless medium, often radio waves, but can make use of wired components as well. With mobile, resource-limited nodes, the network topology is highly dynamic as components may enter, leave, and change position without notice. Such a loosely-regulated system has many potential points of failure, but also a wide range of applications.

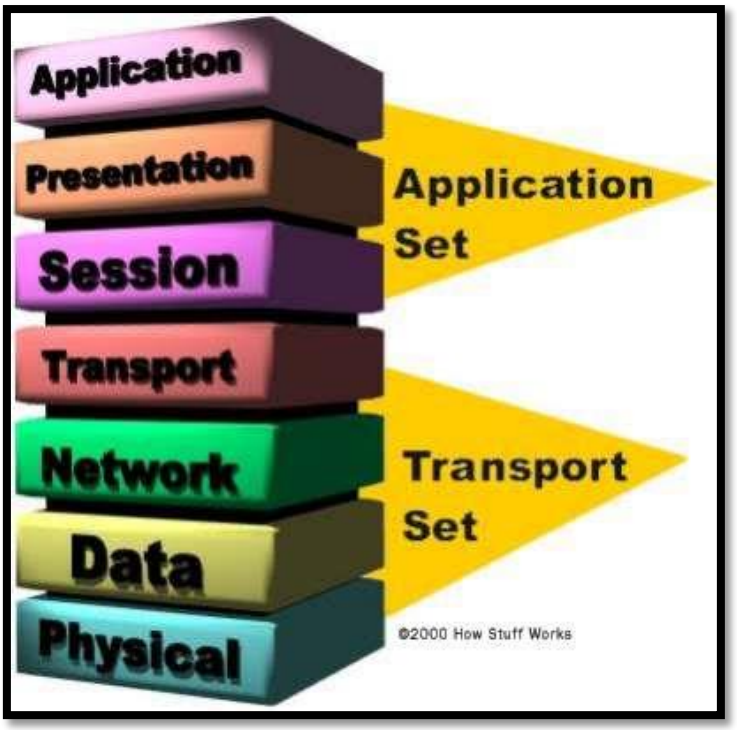
Mobile ad-hoc networks are valuable because they do not require wired infrastructure, can be deployed quickly and/or in hostile environments, and are built of self-contained components. Military communication systems are a primary user of MANETs, allowing soldiers, vehicles, and support equipment to coordinate their actions across the battlefield. This illustration from O'Rourke shows how the military makes use of such a network:



Beyond the military, MANETs can be found in wireless sensor networks, smartphone ad-hoc networks, and vehicular ad-hoc networks (Bluetronics). Wireless sensor networks (WSNs) use environmental monitoring devices to collect data and aggregate it into useful observations. For example, body area networks connect heart-rate monitors, pulse oximeters and other specialized sensors to give a focused view of a person's health. Smartphone ad-hoc networks (SPANs) make use of existing peer-to-peer hardware and software in smartphones to build networks without a central server (Patterson). The case study in this paper, an application called FireChat, uses this technology to create a social network. Vehicular ad-hoc networks

(VANETs) connect vehicles to each other, allowing coordination and traffic information dissemination to improve transportation efficiency. The Vehicular Multi-technology Communication Device under development at Florida Atlantic University is one such VANET (Smart Mobile Computing). When all these disparate MANETs are in place, their intercommunication enables improvements in safety and coordination across society.

The general networking system used by MANETs is the Open Systems Interconnection Model, which is a stack of seven abstraction layers that standardizes communication between computers (Tyson, J.). More specifically, the IEEE 802.11 and related protocols define what the components of a mobile ad-hoc network are and how they communicate. These systems focus primarily on network routing and node connections, so the transport, network, data, and physical layers are covered in this paper's security evaluation (transport set in the image). With the open availability and standardization of networking technology, MANETs have been a popular topic of research, experimentation, and innovative applications.



III. SECURITY VULNERABILITIES IN MANETS

Like all computer networks, mobile ad hoc networks can be subjected to unexpected events. These events may be the actions of an attacker, a hardware or software failure, or an environmental disruption. The basic outcome of any of these scenarios is a denial of service, or DoS, which either limits or stops the network from performing its designed functions. Due to the ad-hoc nature of these networks, even small disruptions to normal service may render the entire deployment effectively useless. When considering security in MANETs, the primary concern is preventing damage from an active attacker, but a robust threat evaluation will also handle general failures under the same protocols. For this reason, all DoS events will be labeled as "attacks," even though they may not necessarily emanate from an actual adversary. Attacks seek to either gain unauthorized access to the network or cause disruption, and exploit weaknesses in the mechanisms that manage the network or provide security. The two main weaknesses of mobile ad hoc networks are their dynamic network topology and lack of central authorization. In this section, common MANET attacks will be discussed and grouped by the layers they target. The names and descriptions of these scenarios are compiled from papers by Wood and Stankovic, Tanwar and Prema, Li and Joshi, and Michiardi and Molva.

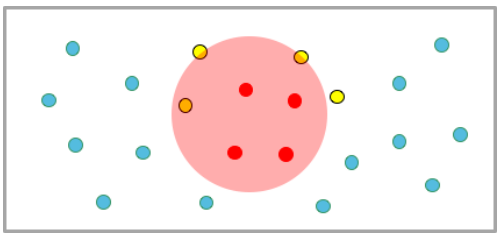
A. Physical Layer

The physical layer encompasses the computing devices that make up the network, the transmission medium that connects these components, and the methods with which signals are sent over this medium. This layer is susceptible to two primary attacks: tampering and jamming.

- Tampering - An attacker may gain access to the machines physically and tamper with them. This could be as simple as destroying the node, or as complex as reverse-engineering it. A node compromised in this kind of attack could be interrogated to reveal network keys and data, or modified to damage the rest of the network. Additionally, tampering and destruction can be indistinguishable from non-attack events. For example, a node being destroyed by an adversary would appear to the

network the same as a node having a total hardware failure. At this level, keeping network components secure depends on hardware design and the deployment environment.

- Jamming - Compared to tampering, jamming is much more likely the result of an active attacker. This kind of attack involves interfering with the communication media – radio frequencies – and preventing successful transmissions. Jamming requires a large expenditure of resources on the part of the attacker, as the energy required to overpower a MANET's signals grows significantly as the range and duration of the DoS increases. The image below shows a jamming attack, with the jammed region in pink. The red nodes are disabled, but the yellow nodes are only partially affected. A smart routing protocol can make use of this to detect jamming attacks and reroute around the area of effect. Therefore, an attack of this type is very difficult to prevent and security designs should be focused on disruption mitigation.



Attacks against the physical layer are external to the network. Although an attacker may use the physical layer to gain access to the MANET's infrastructure, these events do not come from with the within the network components. Security measures, in this case, cannot rely only on communication protocols, but must also include manufacturing and environmental considerations.

B. Data Link Layer

The data link layer is responsible for transferring data between network nodes and converting that data into transmittable frames. The IEEE 802.11 specification divides this into two sublayers, the logical link control (LLC) and the media access control (MAC), controlling data flow and usage of media, respectively. Attacks at this level abuse the cooperative requirements of MANET nodes and work by draining resources. These exploits can come from within the network or originate externally through physical layer vulnerabilities, like jamming. Collision, exhaustion, and unfairness will be discussed as vulnerabilities at the data link layer in a MANET.

- Collision - By inducing errors in data flow control and media access timing, an attacker can overlap frames passing through the data link layer, resulting in a collision. This will invalidate the frames and thus the entire packet, which then requires additional resources to check, invalidate, request retransmission, and resend. The targeted section of the transmission could be as small as a single byte, depending on the strength of the error-correcting system in place, and occur in any part of the message. An adversary using this approach would need only a small amount of power or network access to damage packets, and cause disproportionally large service problems if the network protocols are fully exploited. Protecting against collision is a normal part of network design, so this type of attack can be handled with sufficiently strong error correcting.
- Exhaustion - Taking advantage of the link layer's requirement to resend failed frames, an attacker may drain network and node resources by repeatedly requesting retransmission. Specifically, in the 802.11 protocol, the MAC sublayer uses Request to Send – Clear to Send and Data – Acknowledgement messages to control access to transmission media. A malicious node or collision incident affecting these messages will cause repeated back-and-forth resending until power is depleted. This attack turns the MANET's normal cooperative behavior into a vulnerability, and the protocol functions that handle normal transmission errors cause system failure.

- Unfairness - Probably the most difficult attack to detect and prevent, an unfair node abuses the cooperative nature of a MANET to starve other nodes of their resources. The offender prioritizes its own packets and usage of the link layer over its neighbors, which slows or stops traffic in its section of the network. Immediately effected nodes can also become exhausted trying to gain access to the link layer, which is being hogged by the unfair node. This situation may not necessarily come from an adversary as well; it may simply be the result of conflicting protocol implementations or configurations across nodes. Mitigation of an unfairness attack is a challenge because the event will fall under the normal link layer management schemes and may not be directly addressed by security protocols.

C. Network Layer

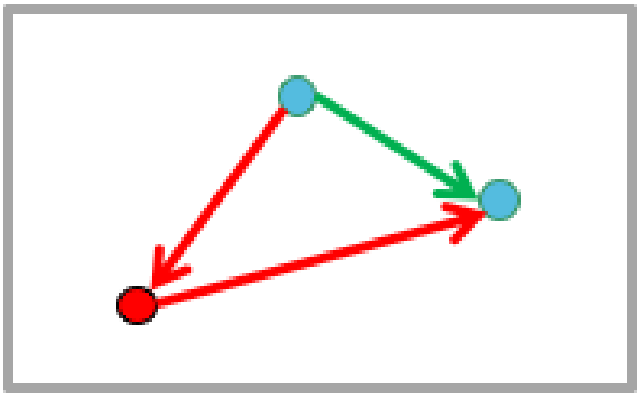
The network layer controls packet forwarding through nodes and handles the routing of the whole network. This layer is vulnerable to a variety of attacks because of its wide range of effect. By targeting the network layer, an attacker can damage or destroy the service to a large number of nodes. In mobile ad hoc networks, the changing network structure and lack of a centralized authorization system make this layer a particularly valuable starting point for adversaries.

- Neglect and Greed - The primary outcome of any attack in the network layer will be to disrupt service to one or more nodes. By manipulating routing messages, a malicious node can appear to be cooperative to lower-level protocols while actually not forwarding messages. This is being neglectful, and such behavior will adversely affect the performance of the network. Similarly, the malicious node may give unfairly high priority to its own messages, which is greedy. Again, the network will suffer with excessive resource consumption by the greedy node and have limited service. Normal routing protocols may not recognize these actions as attacks as well, since routing behaviors may vary across

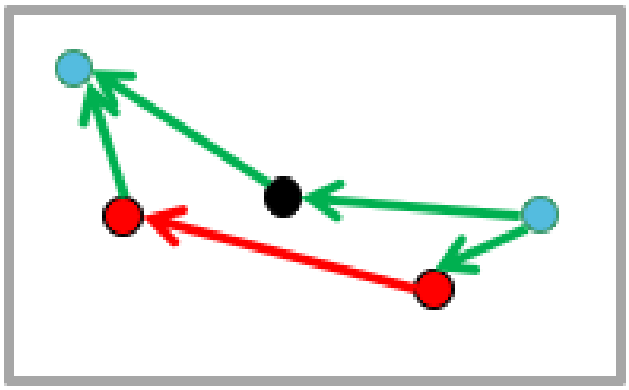
protocol implementations and devices. In MANETs, if no central routing authority is established, neglectful and greedy nodes are very capable of creating denials of service.

- Homing - Although MANETs are generally decentralized and do not have specialized nodes for particular network responsibilities, some implementations may elect to delegate roles, like cryptographic key holders or access points. In a homing attack, an adversary observes network layer actions and identifies these special nodes based on the services they provide. Once a key node or group of nodes has been identified, the adversary can effectively direct other attacks against them. These components can be protected by using an encryption scheme that does not expose their identities.
- Byzantine - One or more nodes may seek to disruption normal network functionality by damaging the network's ability to route packets. This is a Byzantine attack, which is a generalized description of several types of intentionally poor networking. In this scenario, the malicious node or nodes may misdirect routing packets, create loops in routes, mislabel route distances, or perform any other action to cause diminished communication performance. The best defense against these attacks message redundancy, message verification, node monitoring, and network probing. Such measures may not be possible with resource-limited hardware used in MANETs, however.
- Black Hole and Wormhole - By taking advantage of the network's goal of establishing the shortest routes, a malicious node or nodes presenting low distances can gain unfair control over the network. In a black hole attack, the attacker advertises itself as the closest to all nodes, causing all traffic to be directed to itself. Similarly, multiple nodes can work together to create a wormhole, which is a fabricated shortest route. Both methods give the malicious nodes the ability to be neglectful or greedy, or eavesdrop. By sending redundant messages along multiple routes and monitoring the behavior of nodes, black holes and wormholes can be detected and removed.

Black hole – the red node and routes are not optimal, but the victim node is tricked into using them. If multiple nodes are victim, the attacker has control of their messages.



Wormhole – the red nodes work together to make the red route appear optimal. They can then cut out the black node from the network or manipulate other network traffic.



- Spoofing and Sybil - MANET nodes must have a way to identify themselves and other network components, and spoofing and Sybil attacks target these identification schemes. A node that attempts to misidentify itself as another node is spoofing the victim, and its goal is to access messages directed to the spoofed node. In a Sybil attack, one node creates multiple false identities for itself and uses them to gain unfair control of the network. Because these attacks make use falsifying identities, security protocols need authentication and authorization systems for protection.

D. Transport Layer

The transport layer provides node-to-node connections and manages the communication over this connection. At this level, an attacker seeks to disrupt the flow of data from one node to its connected partner. By causing connection errors, reconnections are forced, and resources are drained.

- Flooding - A malicious node may attempt to exhaust a victim by continually requesting connections. The target node is forced to respond to the request and prepare its ports for connection. When no connection is made, more resources are used to reset the node and prepare for another connection. This is a flooding attack; the victim node is flooded with connection requests. Protection from flooding is accomplished by limiting the number of requests a node can make or accept, and is a common feature of MANET protocols. However, Wood and Stankovic present an interesting countermeasure in their paper – puzzles. Any request to connect is met with a puzzle that the requester must solve. If the puzzle is solved, the requester has shown willingness to commit resources to the connection and is unlikely to be attempting a flooding attack.
- Desynchronization - Data flowing from one node to another will likely pass through multiple intermediate nodes, and transport layer works to make this network traversal invisible to communicating nodes. However, the control messages created by this layer are subject to alteration as they pass through the rest of the network. An attack of this manner will cause the connection to desynchronize and require the nodes to expend resources to reconnect. A security system should include an authentication method that prevents message modification, and cryptography to hide the vulnerable parts of connection control packets.

IV. SECURITY OF MANETS

Due to unique nature of Mobile Ad-Hoc Networks and their lack of resources the security is difficult to implement not only due to the networks ever-changing topology but also due to very low resources like power and bandwidth and frequent lack of central authority. Therefore, not all networks have all security measures implemented; however, all security solutions try to be low resource cost and scale across networks sizes and bandwidths, adopt to normal network errors, and be available for all network components at all times (Maghoub).

A. Physical Secuirity through FHSS and DSSS

Frequency Hopping Spread Spectrum is a method of transmitting radio signals by switching carrier quickly among many frequencies using sequence known to both transmitter and receiver. FHSS is mostly deployed to protect wireless communication from eavesdropping, jamming, and other interference by increasing dimensional characteristics of the transmitted signal. Signals of spread spectrum are indistinguishable from background noise making it much harder to detect but it comes at cost of high complexity and higher transmission cost (Ebrahimzadeh & Falahati).

Direct Sequence Spread Spectrum is a technique whereby the original data signal is multiplied with pseudo random noise spreading code. Spreading code has higher chip rate which results in wideband time continuous scrambled signal (Han). The energy of the original signal is spread into much higher bandwidth and the receiver can reconstruct the original signal by multiplying the received signal by same spread code. The sender first transforms the message to a sequence by replacing each 0 with -1 therefore the signal transmitted is composed of positive and negative ones and then this sequence is converted to RF signal. This is very effective anti-jamming technique widely used in CDMA systems (Zhang et al).

B. Data Link Layer Secuirty through ERA 802.11

ERA 802.11 is an algorithm that ensures randomness in ad-hoc networks and the detection system is used to monitor nodes for selfishness. In case of misbehavior a report is sent to an external reputation management system. Protocol depends on encryption methods which need additional computation that lead to overhead. ERA-802.11 adds additional messages in its protocol; therefore, it is not compatible with 802.11 standard (Santhanam et al).

C. Network Layer Security through HMAC and Digital Signature

Hashed Message Authentication Code methods are based on nodes sharing symmetric key which can be efficiently generated and verified though one way hash function. The message can only be verified by the receiver and establishing the secret key between two nodes is simple and Secure Routing Protocol is used to distribute the shared keys (Maghoub). On the other hand Digital Signature uses asymmetric key cryptography and involved much more computation for all the operations around decryption and encryption of the message. It is also much less resistant against denial of service attacks due to its high computation cost and therefore it could be very easily overwhelmed with by large number of signatures (Wood & Stankovic).

D. Black Hole Attack Security through SAR

Secure Aware Ad-Hoc Routing Protocol defines level of trust as metric for routing and uses key distribution or secret sharing mechanism. In the intermediate nodes if trust level is satisfied the node will proceed to transmit route request. SAR is using Ad-hoc on Demand Distance Vector protocol for encryption and decryption process using common key (VinothKumar & Rajaram). SAR may experience transmission delays due to its use of AODV as new routing path will be sought as soon as data transmission fails. Additionally during the new routing path search connection may not be found as security level of intermediate node may be lower than protocol dictates (Han)

E. Impersonation Attack Security through ARAN

Authenticated Routing for Ad Hoc Networks is a security protocol based on cryptographic certificates which overcomes all types of attacks in the network layer. Three major properties of cryptography, authentication, integrity, and non-repudiation which are supported with both Dynamic Source Routing and Ad-Hoc on Demand Distance Vector protocols. ARAN provides authentication and non-repudiation services using predetermined cryptographic certificates for end-to-end authentication. Each hop verifies the signature of the previous hop and replaces it with its own. Additionally, ARAN uses trusted certificate server where each node has to request certificate signed by such server (Sanzgiri et al).

F. Modification Attack Security through SEAD

Secure Efficient Ad Hoc Distance Vector Routing protocol is based on the design of the Destination-Sequenced Distance-Vector routing protocol and it can overcome denial of service, routing attacks, and resource consumption attacks. It uses one way hash function without the usage of asymmetric cryptographic mechanism. The mechanism uses authentication to differentiate between malicious and non-malicious nodes, which in turn reduces resource consumption attacks launched by malicious nodes. Because different hash function is used for different variables used, the attacker can never forge lower metric value, or greater sequence value (Hu).

G. Trust in Ad-Hoc Networks

Trust and Key Management is critical supporting element of any security system. Its basic operations include establishing trust and secret connection as well as key exchange and update. Keys use both symmetric and asymmetric cryptographic functions for authentication, confidentiality, and integrity. There are three methods of establishing and monitoring trust in ad-hoc networks: trusted third party, web of trust, and localized trust. Trusted third party uses certification authority that is trusted by every node and all nodes that

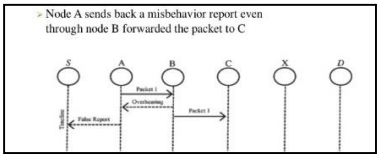
are considered trustworthy by this authority are trusted by every node in the network. This is highly centralized scheme and it employs threshold cryptography to distribute private keys among server nodes while making public key available to every node. This system can create a bottle neck for large networks and it is vulnerable to denial of service attacks. Web of trust is a polar opposite of the trusted third party as no particular structure exist and schema is highly decentralized. Each node manages its own trust based on direct communication with other nodes. The system is built on top of direct communication via secure side channels and nodes that have established security associations with immediate neighbors also trust other nodes with who their neighbors established same level of security. Finally, last method is called Localized Trust which is a mix of both systems where node that is trusted among other nodes may become certification authority for other local nodes. Localized trust pattern of security minimizes its impact on network scalability and performance while maximizing security (Ilyas & Mahgoub).

H. Localization Detecttion, End Host Reaction, Watchdog, and Pathrater

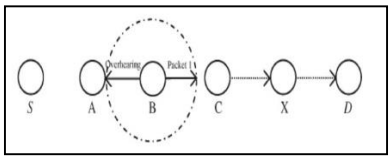
Localized Detection uses Watchdog to monitor packet forwarding on top of source routing protocols like Direct Source Routing and it assumes symmetric bidirectional connectivity. Because the whole path is specified, when node forwards a packet to the next hop, it knows following next hop. It then overhears the channel for transmission and if it does not hear the transmission after a time-out, a failure tally associated with node is increased. If the tally exceeds a threshold bandwidth, source sends a report packet to the source notifying other nodes misbehavior. End Host Reaction uses Path Rater which allows each node to maintain its own rating for every other node that it knows about. A node slowly increases the rating of well-behaving nodes over time, but dramatically decreases the rating of a malicious node that is detected by its Watchdog. Based on the rating, the source always picks up a path with highest average rating. Watchdog and Path Rater are two main components that try to improve performance of Ad-Hoc networks in presence of disruptive nodes. Watchdog determines behavior by copying packets to be forwarded into a buffer and

monitoring the behavior of the adjacent nodes of these packets. Watchdog snoops to decide if the adjacent node forwards the packets without modification. The number of violation is compared to a predetermined threshold before the node is marked as suspicious. Path Rater on individual node works to rate all of the known nodes in particular network with respect to their reliabilities. Ratings are made and updated from particular node perspective. There are three issues with watchdog which are false misbehavior, limited transmission power, and receiver collision.

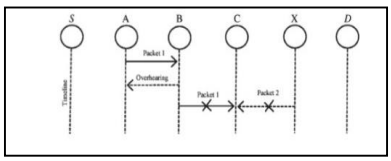
False behavior issue happens when malicious node intentionally claims that other nodes are malicious and misbehaving.



Limited transmission power happens when source node overhears neighbor node which sent data to another node but that node did not receive it due to adjustment of transmission power while transmitting.



Receiver collision issue happens when source node cannot tell if neighboring node sending packets to another node were received (Nadeem & Howarth).



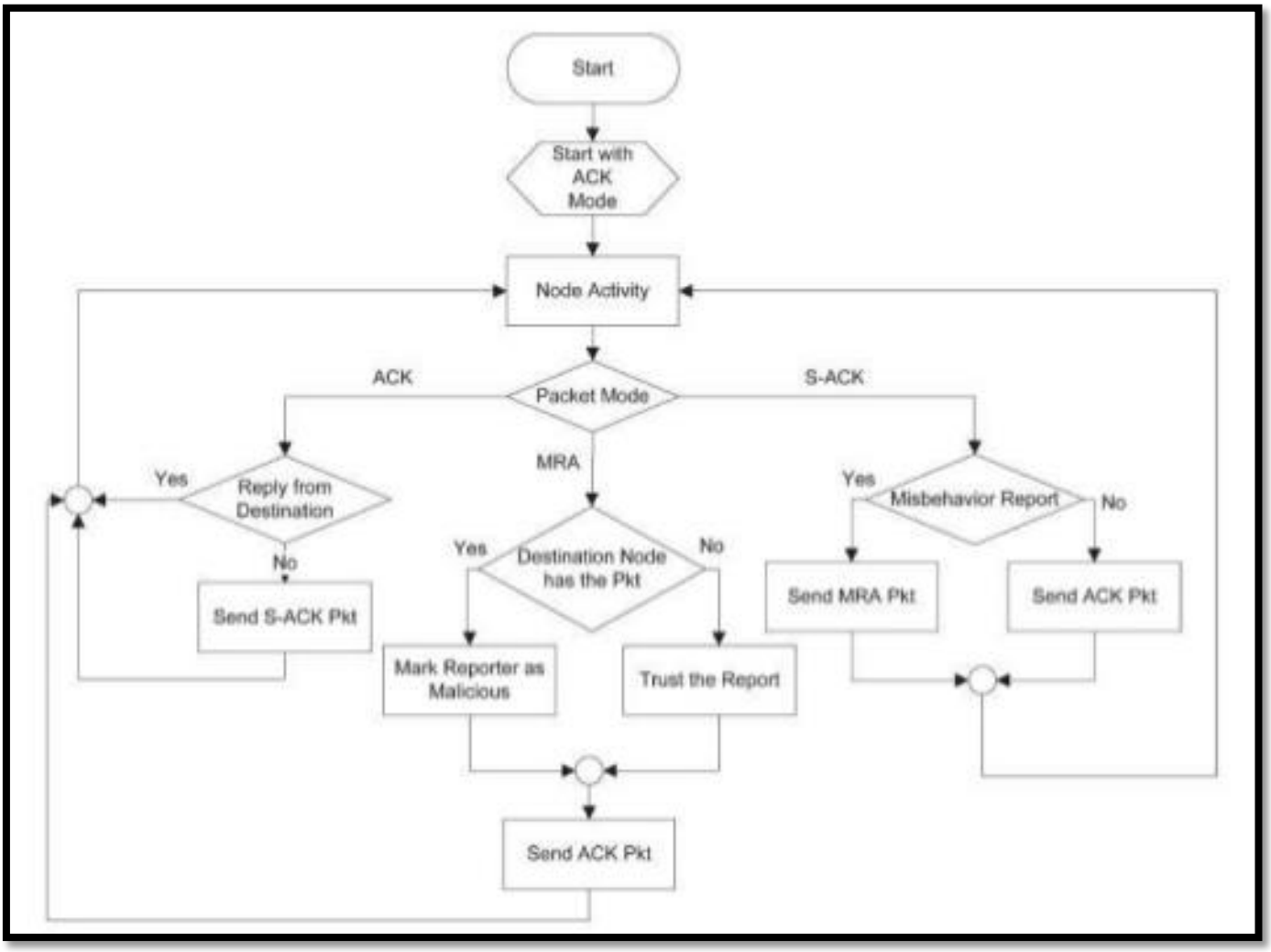
I. Global Reaction, ACK-Based Detection, and TWOACK

Global reaction scheme is based on the ubiquitous and robust access control framework. Once multiple nodes in a local neighborhood have reached the consensus that one of their neighbors is malicious, they collectively revoke the certificate of the malicious node. ACK fault detection mechanism is based on explicit acknowledgments. The destination sends back acknowledgements to the source for each successfully received packet. The source can initiate a fault detection process on a suspicious path that has recently dropped more packets than an acceptable threshold. It performs a binary search between itself and the destination and sends out data packets piggybacked with a list of intermediate nodes, also called probes, which should send back acknowledgements. TWOACK which is Two Network Layer Acknowledgment protocol detects misbehaving nodes and seeks to alleviate the problem by notifying routing protocol to avoid them in the future routes. The protocol monitors source, intermediate, and destination nodes and keeps the counter that this incremented after each packet transmission and monitors the node for transmission time and accuracy of transmission. If transmission time is longer than expected node is marked as misbehaving and if transmission differs from original packet then confidentiality is lost. TWOACK addresses two issues with watchdog method which are receiver collision and limited transmission power; however, it carries much larger overhead than Watchdog and Pathrater method (Balakrishnan & Deng & Varshney).

J. Enchanced Adaptive Acknowledgment EAACK

Enhanced Adaptive Acknowledgment protocol addresses all three problems that occurred with Watchdog method and it is based on TWOACK scheme and it has an acknowledgment based network layer scheme which can be used as a combination of TWOACK and End to End acknowledgment scheme called ACK. EAACK is composed of three major parts: ACK, S-ACK which is improved version of TWOACK, and Misbehavior Report Authentication. Compared to TWOACK this protocol considerably reduces network overhead while still capable of maintaining and even surpassing the same network throughput during data

transmission. The end to end transmission sends a packet without overhead except for a flag indicating packet type. In this network all intermediate nodes simply forward this packet to next nodes. When destination node receives the packet it sends back an acknowledgment packet to the sender down the reverse order of the same route. That's how accuracy of the packet transmission is determined. MRA detects misbehaving nodes with the presence of the false misbehaving report (Shakshuki & Kang & Sheltami).



V. CASE STUDY

Although mobile ad-hoc networks can provide a variety of specialized uses, their deployments are still limited due to the relative newness of the technology and the risks of security failures. Outside of the military, few civilian applications of MANETs are found in scientific literature. However, recent news stories have covered an application the does make use of mobile ad-hoc networking – FireChat. The application is available on iOS and Android smartphones, and is used to create a social network without completely relying on cellular infrastructure. Users share their Bluetooth and Wi-Fi connectivity, then join local area chatrooms or send direct messages. The technology employed is not publicly available, but does make use of iOS's Multi-peer Connectivity Framework (McGarry) and possibly Android's Linux Wireless Extension. Since its release in 2014, it has proven popular in areas where Internet connections are poor or subject to governmental oversight. In particular, FireChat received a great deal of coverage during the 2014 Taiwan Umbrella Protests, where activists used the app to organize without being subject to censorship and observation.

The security issues faced by FireChat have not been released to the public, but users report problems similar to those present in any mobile ad-hoc network (Tyson, G.). Because the ad-hoc social network is not moderated, anyone can join, including malicious actors. Furthermore, without an authentication system, posing as another person is as easy as typing in the victim's name. In a potentially dangerous environment, anyone using the app also risks physical attack, like a node in a MANET. There are encryption features available, and users can establish their own systems for authorization and authentication in the chatrooms, but this can be difficult if coordinating thousands of people. Despite these challenges, FireChat has proven itself invaluable to people who need to communicate in areas of poor infrastructure or oppressive organizations.

VI. CONCLUSION

Mobile ad-hoc networks offer a wide range of applications, but struggle to overcome the primary challenge of security. This is not only preventing private information from being exposed, but also includes any diminished functionality of the network. Because of the resource limitations placed on these networks, implementing an effective security system is difficult, if not impossible. However, with smart protocol implementation and continual improvement, MANETs will find use in more and more areas. The current state of development has a variety of open source methods for securing communications, which is essential to good security – the algorithm is public, the key is private. Alongside robust protocols, the hardware of network components must get better. Batteries need to last longer, transmitters need to be stronger, and physical components need to be tamper-resistant. Real-world deployments are limited, but as the technology continually matures, mobile ad-hoc networks will become the dominant application of computing power in the future.

VII. REFERENCES

Balakrishnan, K., Deng, J., & Varshney, V. K. (2005). TWOACK: Preventing selfishness in mobile ad hoc networks. Paper presented, 4 2137-2142 Vol. 4. doi:10.1109/WCNC.2005.1424848

Bluetronics. "Mobile Ad Hoc Networks." N.p., n.d. Web. 09 Apr. 2016. <http://www.bluetronix.net/mobile_ad_hoc_ networks.htm>.

Ebrahimzadeh, A., & Falahati, A. (2013). Frequency hopping spread spectrum security improvement with encrypted spreading codes in a partial band noise jamming environment. Journal of Information Security, 4(1), 1. Retrieved from http://ezproxy.fau.edu/login?url= http:// search.proquest.com/docview/1718944448?accountid=10902

Han, I., Ryou, H., & Kang, S. (2006). Multi-path security-aware routing protocol mechanism for ad hoc network. Paper presented, 1 620-626. doi:10.1109/ICHIT.2006. 253556 "The History and Evolution of Cell Phones." The Art Institutes Blog. N.p., n.d. Web. 09 Apr. 2016. <https://www.artinstitutes.edu/blog/the-history-and-evolution-of-cell-phones>.

Hu, Y. (2003). SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks. Ad Hoc Networks, 1(1), 175-192. doi:10.1016/S1570-8705(03)00019-2

Ilyas, Mohammad, and Imad Mahgoub. Mobile Computing Handbook. Boca Raton: Auerbach Publications, 2005. Print.

Li, Wenjia, and Anupam Joshi. "Security Issues in Mobile Ad Hoc Networks- A Survey." CiteSeerX, n.d. Web. 25 Mar. 2016.

Mahgoub, Imad. "Introduction to Mobile Computing." Florida Atlantic University. Lecture.

McGarry, Caitlin. "How FireChat Is Using an Obscure IOS Feature to Change Messaging." PCWorld. N.p., 31 Mar. 2014. Web. 03 Apr. 2016. <http://www.pcworld.com/article/2137265/how-firechat-is-using-an-obscure-ios-feature-to-change-messaging.html>.

Michiardi, Pietro, and Refik Molva. "AD HOC Networks Security."Basagni/Ad Hoc Networking Mobile Ad Hoc Networking (2005): 329-54. Web.

Nadeem, A., & Howarth, M. P. (2013). “A survey of MANET intrusion detection & prevention approaches for network layer attacks.” IEEE Communications Surveys & Tutorials, 15(4), 2027-2045. doi:10.1109/SURV.2013. 030713.00201 O'Rourke, Chris. "COTS Journal." Mobile Ad Hoc Networking Revamps Military Communications - N.p., Nov. 2011. Web. 03 Apr. 2016.
<http://www.cotsjournalonline.com/articles/view/102158>.

Patterson, Stephen Max. "Android Phones Are Connecting without Carrier Networks." Network World. N.p., 12 Feb. 2013. Web. 03 Apr. 2016. <http://www.networkworld .com/article/2224025/smartphones/android-phones-are-connecting-without-carrier-networks.html>.

Santhanam, L., Xie, B., & Agrawal, D. (2008). “Selfishness in mesh networks: Wired multihop MANETs.” IEEE Wireless Communications, 15(4), 16-23. doi:10.1109/MWC.2008.4599217

Sanzgiri, K., LaFlamme, D., Dahill, B., Levine, B. N., Shields, C., & Belding-Royer, E. M. (2005). “Authenticated routing for ad hoc networks.” IEEE Journal on Selected Areas in Communications, 23(3), 598-610. doi:10.1109/JSAC.2004.842547

Shakshuki, E. M., Kang, N., & Sheltami, T. R. (2013). “EAACK-A secure intrusion-detection system for MANETs.” IEEE Transactions on Industrial Electronics, 60(3), 1089-1098. doi:10.1109/TIE.2012.2196010 "Smart Mobile Computing | FAU Tecore Networks Lab." Smart Mobile Computing. N.p., n.d. Web. 09 Apr. 2016. <http://smc.eng.fau.edu/>.

Stojmenović, Ivan. Handbook of Wireless Networks and Mobile Computing. New York: Wiley, 2002. Print.

Tanwar, Sarvesh, and Prema K.V. "Threats & Security Issues in Ad Hoc Network: A Survey Report." International Journal of Soft Computing and Engineering (IJSCE) 2.6 (2013): n. pag. Web.

Tyson, Gareth. "Mesh Networks and Firechat Make 'switching off the Internet' That Much Harder." Phys.Org. N.p., 7 Oct. 2014. Web. 01 Apr. 2016. <http://phys.org/news/ 2014-10-mesh-networks-firechat-internet-harder.html>.

Tyson, Jeff. "How OSI Works." HowStuffWorks. N.p., n.d. Web. 25 Mar. 2016. <http://computer.howstuffworks. com/osi1.htm>.

VinothKumar, K., & Rajaram, A. (2014). “An efficient security aware routing protocol for mobile ad hoc networks.” International Journal of Computer Science and Network Security (IJCSNS), 14(12), 66.

Wood, A.D., and J.A. Stankovic. "Denial of Service in Sensor Networks."Computer 35.10 (2002): 54-62. Web.

Zhang, R., Sun, J., Zhang, Y., & Huang, X. (2015). “Jamming-resilient secure neighbor discovery in mobile ad hoc networks.” IEEE Transactions on Wireless Communications, 14(10), 5588-5601. doi:10.1109/ TWC.2015.2439688