Mobile Ad Hoc Networks in a Zero Trust Architecture for the Tactical Edge

Dane Oshiro
Naval Postgraduate School
dane.oshiro@gmail.com

Alan Shaffer
Naval Postgraduate School
alan.shaffer@nps.edu

Gurminder Singh
Naval Postgraduate School
gsingh@nps.edu

Abstract

Mobile Ad Hoc Networks (MANETs) are resilient and responsive networks capable of supporting the unique requirements at the tactical edge. MANETs can provide critical support at the tactical edge of military operations but the current Department of Defense (DOD) strategy for Zero Trust Architecture (ZTA) does not include guidelines for MANET implementation. The connectivity between users, devices, sensors, and shooting platforms in the information-age battlefield increases the attack surface for adversaries to penetrate these forward-edge networks. Additionally, solutions at the forward edge must be sensitive to the considerations of bandwidth, processing, and power consumption. In this paper, we introduce a set of ZTA requirements that complement MANET secure routing protocols and intrusion detection systems. We survey several MANET routing protocols to identify ones that can be augmented to achieve zero trust principles in the network. This survey leads to identifying the Zone-Based Intrusion Detection System (ZBIDS) running on a hybrid routing protocol as a security solution that can be incorporated into a ZTA.

1 Introduction

Mobile ad hoc networks (MANETs) configured using a traditional defense-in-depth (DiD) security approach at the tactical edge pose significant security risks unless key zero trust (ZT) concepts are incorporated during system design and throughout operational use. MANETs are self-organizing and decentralized wireless networks that do not require a central authority to establish an infrastructure for network connectivity [1]. Each node within a MANET is capable of routing packets to other nodes within the network. This infrastructure-less approach to networking makes a DiD security implementation very difficult. This is because the DiD security model organizes several network protection devices relative to a perimeter, delineating domains with varying levels of trust [2]. The problem with applying such a model to a MANET is that there is no perimeter that separates nodes from one other. This lack of a perimeter and trusted domains makes MANETs uniquely suited to incorporating ZT principles. These principles rest on three fundamental concepts introduced by Kindervag and Balourous [3]. The first concept assumes that all traffic is untrusted; the second promotes the implementation and enforcement of granular access control; and, the final concept advocates for the inspection and logging of all network traffic to provide security managers with real-time situational awareness of their networks. An implementation of these concepts is achieved in a comprehensive zero trust architecture (ZTA).

This paper first introduces the relationship between ZT concepts and the tactical environment. Next, we explore the fundamental components within a ZTA and their associated implementations at the tactical edge. Then we present several challenges associated with ZTA implementations of tactical ad-hoc networks and MANETs. Finally, we introduce a set of implied requirements for MANETs in a tactical edge ZTA.

2 Zero Trust in the Tactical Environment

The first concept of ZT assumes that all network traffic is untrusted. Traditionally, networks rely on the concept of a trusted internal network perimeter [4], assuming that any traffic originating within the perimeter is legitimate and safe. The technological capabilities of nation-state actors challenge the permeability of such perimeters. The increasing connectivity between users, devices, sensors, and weapons platforms in the information-age battlefield increase the attack surface for adversaries to potentially penetrate these forward-edge networks. Network intrusion needs to be assumed in the design of future tactical networks. The bandwidth and processing power available at the tactical edge are limited in comparison to an enterprise setting. Given the assumption of intrusion and these limitations, resources should ideally be focused on protecting data rather than only hardening the network. Under a traditional network-centric approach, a network breach would

necessitate the move from primary methods of communication, such as on a federated chat server, to secondary communications links, such as radio voice communications. Rather, a tactical network must employ an approach to security that provides commanders with the ability to isolate malicious nodes on the network, while preserving the availability of warfighting services.

The second concept of ZT is the enforcement of granular access controls on the network. This can be achieved by implementing policies that enforce and govern access control, restricting resources that are available to users and devices based on the needs of their authorized tasks. For example, a user dealing with casualty evacuation and other medical service support applications should not be able to open data logs for fire missions. If a user with a medical service role becomes compromised in a ZT network, the only resources that an attacker would be able to access are those that deal with medical information, and perhaps only those associated with that role. The granular access control policies mitigate the potential for widespread information leakage in a network from a single compromised user or device.

Enforcement of these policies is done through a variety of continuous authentication (CA) mechanisms. These mechanisms elevate the security posture of networks employing Single-Sign-On (SSO) by not granting users access to all system resources after logging in only once on the network [5]. The one-time authentication of SSO creates a single point of failure in a security architecture. Although Multi-Factor-Authentication schemes [6] raise the barrier for network intrusion, a CA approach provides a persistent security presence within the architecture. Some of these approaches incorporate location-based data gathered from devices as mentioned in [7], while some use behavioral methods such as keyboards strokes [8], [9], or user gait analysis using mobile devices [10]. Some of these CA methods focus on authentication based on telemetric data captured from networking components [11]–[14] to authenticate devices.

Using a mix of continuous authentication mechanisms across a variety of schemes provides tactical networks with a durable authentication framework that removes the single point of failure in a security architecture. These can also potentially reduce the communication overhead requirements associated with SSO implementations, such as the need to refresh certificates with servers located outside of the tactical network. Reducing the amount of traffic for external communications lowers the electromagnetic signature of tactical networks, lowering the probability of detection by adversarial electronic warfare units.

The final concept of ZT deals with the logging and inspection of all network traffic. Being able to locally log and inspect traffic provides tactical networks with the ability to deploy local instances of intrusion detection systems (IDS), reducing the response time it takes to recognize malicious users on a network[15]. Auditing and logging actions for all agents on a network generates a vast amount of data. Analysis of logs for every user, device, and service on the network forms a baseline of each agent's respective behavior. Efficient storage and analysis of these logs can be bolstered through applications of machine learning to inspect traffic and refine policies. Such algorithms have successfully been implemented on web application firewalls in [16] but have yet to be tested in a tactical environment. Deploying organically hosted IDS reduces the requirement to send these logs back to the enterprise environment for further analysis. Decreasing external network traffic serves to further minimize the electromagnetic footprint of units at the tactical edge.

The three fundamental concepts discussed above illustrate the benefits of ZT in a tactical network. A ZT tactical network is resilient to network intrusion, has built-in mitigations against a compromised user, and can potentially have a lower electromagnetic signature. All of these require adoption of a ZTA, with several components that enable these capabilities at the tactical edge.

3 Zero Trust Architectures at the Tactical Edge

The comprehensive framework that operationalizes concepts introduced in ZT is the Zero Trust Architecture (ZTA). Based on the limitations of processing power and communication bandwidth resources available at the forward-edge, some components of a ZTA will need to be hosted on both tactical and enterprise networks. The Department of Defense (DOD) recognizes seven pillars necessary for any ZTA implementation [17], [18]. These pillars, as depicted in Figure 1, are: Users; Devices; Applications and Workloads; Data; Network and Environment; Automation and Orchestration; and Visibility and Analytics.

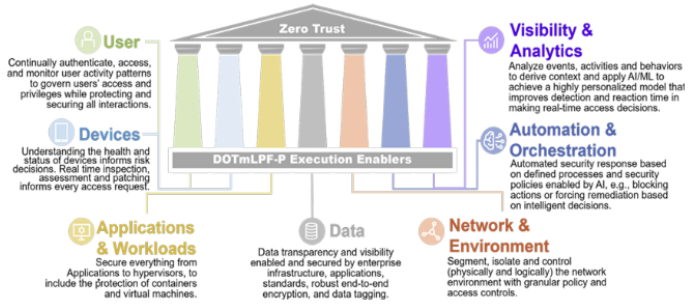

Figure 1: DOD Zero Trust Pillars from [17]

A tactical ZTA implementation must be able to address every pillar with reduced resources, in a mobile environment, and be able to continue to deliver ZT capabilities in a degraded or disconnected environment. The three main logical components of a ZTA introduced in [17], [18] are the Policy Engine (PE), Policy Administrator (PA), and Policy Enforcement Points (PEPs). Together, these components govern granular access control for all resources within the ZTA. The PE computes a trust score for every agent on its network using metadata collected from PEPs. The PA determines the set of available resources to an agent based on its trust score. Finally, PEPs enforce the access between agents and system resources. Although the process requires additional logging and metadata to be passed within the network, the presence of a local PA, PE, and PEPs reduce the requirement to transmit this data on resource-constrained external communication links.

The heterogeneity of devices present at the tactical edge also presents a unique requirement as some devices will not be compatible with ZTA components. Devices that are incompatible with one another and that are unable to be modified are called legacy devices (LD). An example of an LD operating on a tactical network is a loitering munition, which may not have the ability to interface with a local PEP. One method to incorporate such LDs into a ZTA framework is to adapt the legacy component architecture from "Zero-Trust Principles for Legacy Components" [19] that addresses LDs present in industrial control systems.

In summary, implementation of a tactical ZTA differs from enterprise solutions. Solutions at the forward edge must be sensitive to the considerations of bandwidth, processing, and power consumption. There is also a need to limit electromagnetic signatures through the incorporation of logical components and cope with the prevalence of heterogenous LD.

4 Mobile Ad Hoc Networks

This section lays out the basic concepts for proposing a set of requirements for a MANET within a tactical edge ZTA. A brief survey of MANET routing methodologies introduces the significance of scalability and performance of these protocols. Additionally, this section delves into the implementation of security features in various routing protocols within MANETs. These protocols contribute to a foundational level of security in a MANET.

Ad hoc networks are decentralized networks with the ability to organize nodes to form a self-configuring and self-healing network topology. Each node in an ad hoc network can perform routing functions, such as determining the most efficient paths between nodes. A traditional network relies on a centralized architecture with fixed infrastructure such as base stations or access points that determines routes. If a base station or access point of a traditional network fails, or is compromised or destroyed by adversaries, nodes on that sub-network, or potentially the network as a whole, may no longer be able to connect to each other. An ad hoc network does not share this critical vulnerability. The network will still function even if a large number of nodes are compromised. Routes using compromised nodes will be discarded, isolating malicious nodes on the network. This distributed approach to routing makes ad hoc networks ideal for use at the tactical edge.

Two prominent types of ad hoc network are vehicular ad hoc networks (VANETs) and mobile ad hoc networks (MANETs). The main difference between the two is the incorporation in a VANET of roadside infrastructure that can communicate with vehicles [20]. The main feature of a MANET is that networking between nodes does not require fixed or permanent infrastructure [1].

The principal methods for determining routes between nodes in a MANET include proactive or reactive [1]. Proactive methods share similarities with traditional networks which rely on propagating source-destination pairs between every node available on the network. Every node in a proactive approach maintains up-to-date routing information to every other node in the network. Examples of proactive protocols are Wireless Routing Protocol [21] and Destination-Sequenced Distance Vector (DSDV) routing protocol [22]. Although proactive methods ensure that every node has the most efficient route to every other node on the network, these protocols tend to generate a large amount of overhead network traffic [23]. In contrast, reactive methods determine routes only when a node requests a route to another node. Examples of reactive protocols are Ad hoc On-Demand Distance Vector (AODV) [24] and Dynamic Source Routing [25]. The on-demand nature of the protocol reduces the communication overhead but comes at the cost of increased latency when determining routes.

Every protocol based on proactive and reactive methods satisfies basic routing requirements in a MANET. However, both methods suffer from limitations that hinder scalability. A performance comparison between a reactive (AODV) and proactive (DSDV) methods confirmed that both protocols suffer from dropped packets (reactive) or delays from network saturation (proactive) even when scaled to a modestly sized

fifty-node network [26]. While these protocols demonstrated effectiveness in smaller network environments, achieving scalability in a MANET necessitates a hybrid approach that combines the strengths of both methods. By integrating the two approaches, it becomes possible to optimize performance and minimize delay, resulting in a more robust and scalable MANET routing solution.

A solution that combines proactive and reactive methods is called hybrid routing. An example of hybrid routing protocols is the Zone Routing Protocol (ZRP) [27]. The network topology is segmented into distinct zones when ZRP is used. Each node proactively maintains routes within its local zone. Any traffic that requires a route between zones is determined using a reactive method. The combination of the two methods reduces the communication overhead between zones while simultaneously reducing the delay to determine routes to neighboring nodes. Scalability is achieved by effectively tuning the routing zone radius, which can minimize the volume of communication overhead within a MANET. A performance analysis of ZRP concluded that it outperforms both proactive and reactive methods in terms of scalability [28].

ZRP is a scalable routing protocol, but it lacks robust security features. Some of the most common types of security risks associated with MANETs are Denial of Service (DoS), black holes and impersonation. A DoS attack takes advantage of the limited bandwidth available on MANETs, generating numerous route request packets to all the other nodes on the network. The saturated network reduces the bandwidth available for data flow and other legitimate route requests on the network, increasing network latency. Black holes are a subset of DoS attacks [29]. Malicious nodes respond to every route request on the network with a route reply indicating that the malicious node contains the shortest route to every request. Once all other nodes have mapped the malicious node as the shortest path to every other node on the network, the malicious node drops every packet sent to it. As a result, no legitimate packets reach their destination. Additionally, unencrypted MANETs are especially vulnerable to eavesdropping from malicious users with compatible radio transceivers [30]. After collecting enough traffic, it may be possible for a malicious actor to impersonate or even hijack a legitimate node if strong authentication mechanisms are not employed [31]. These security concerns highlight that MANETs are vulnerable to attacks that compromise the confidentiality and availability of data.

Several security solutions improve the confidentiality and availability of MANETs. Encryption schemes such as hashed message authentication codes (HMAC) can be applied to routing protocols to prevent eavesdropping and impersonation on the network. An example of a routing protocol that uses HMAC is the security enhanced zone routing protocol (SEZRP), which uses an a priori approach to key distribution before nodes are deployed [32]. Distribution of keys before node deployment reduces communication overhead in a bandwidth constrained environment. An analysis of SEZRP using a Network Simulator version 2 (NS2) indicated that the protocol had a negligible delay compared to ZRP and improved the average throughput of a MANET when up to twelve malicious nodes were inserted into the network [32].

Another security solution that improves confidentiality segregates the type of encryption used based on the type of network traffic; this protocol is called secure zone routing protocol (SZRP) [33]. An asymmetric encryption scheme facilitates security of control data traffic such as route requests and route replies by preventing eavesdropping. Nodes sign and verify route requests and route replies using public and private keys between each node. Data packets are encrypted using symmetric keys. Authentication between nodes uses asymmetric keys when routes are determined in the MANET. This scheme prevents eavesdropping, man-in-the-middle or impersonation attacks from occurring on the network. An impersonating node will need a legitimate node's private key to sign and verify control packet information. The incorporation of an asymmetric encryption scheme enables encrypted data exchange without the need to share or distribute a common key throughout the network.

The application of an asymmetric encryption scheme unfortunately incurs a performance cost at each node. Processing every control packet using signing and verification at each node is computationally more expensive than encrypting and decrypting packets using a symmetric key. A study using Network Simulator version 2 (NS2) revealed that a SZRP implementation increased the average size of packets by 183% and increased latency by 146% delay in larger networks[34].

Although both solutions increase confidentiality of a MANET, neither solution addresses security concerns that affect availability. Two security solutions enhance availability in ZRP [35]. One solution by Soms et al. in [36] is zone-based intrusion detection system (ZBIDS). Each node in a ZBIDS architecture employs an intrusion detection system (IDS) agent that observes other nodes within their respective zones for misbehavior. Behavior of

nodes are observed using an enhanced adaptive acknowledgement (EAACK) scheme [37], which validates route paths after packets are sent to a destination. A source node in a benign MANET should expect acknowledgement packets from a destination node that follow the same route the outgoing packets traveled, but in reverse order. Should discrepancies arise, every three nodes along the route will attempt to detect where the misbehaving node is on the MANET. Once the misbehaving node is identified, a misbehavior report authentication (MRA) packet is sent to the destination node using an alternative route from source to destination. Since the malicious node is circumvented when the MRA packet is sent, it is not possible for a malicious node to send a MRA packet, which must be sent by a legitimate source node. A graphic depiction of the EAACK scheme is illustrated in Figure 2. The nodes that perform interzone communication also perform EAACK using reactive protocols. The additional packets used to determine where a black hole exists on a MANET increases the number of packets that need to be sent between nodes.

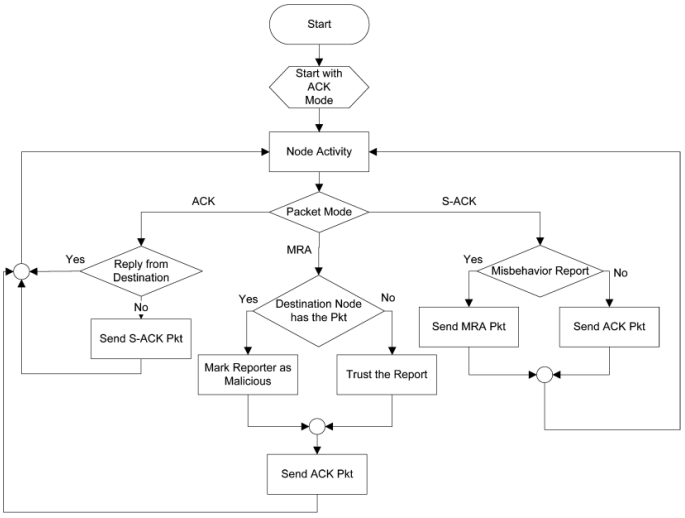

Figure 2: Enhanced Adaptive Acknowledgment (EAACK) Intrusion Detection Scheme from [37]

The second method that enhances availability in a hybrid routing protocol uses a fuzzy logic model to compare two parameters to determine a path [38]. The first parameter reflects the reliability of a node by observing its ratio of successfully forwarded and dropped packets. The second parameter determines the centrality of a node within its zone. A node with many dropped packets and high centrality are indicative that the node potentially a black hole. No study has been conducted on this method to determine its communication overhead requirements, but both parameters could be determined through in-line methods for examining packet metadata.

In summary, several MANET routing methods and protocols were introduced in this section. Proactive and reactive methods serve as the building blocks for developing hybrid routing approaches. Breaking the network topology into zones allowed ZRP to take advantage of both proactive and reactive routing methods. Low latency intra-zone networking is achieved through maintenance of routing tables for all nodes in a zone. Communication overhead is reduced for inter-zone traffic since route request/route reply packets are only sent when a new destination is requested.

Additionally, several security concerns relevant to MANET routing were introduced. Confidentiality and availability within a MANET are vulnerable from several types of attacks. The principle of confidentiality is susceptible to eavesdropping and impersonation attacks. Availability is another key consideration due to the already constrained communication pathways that are inherent to MANETs, which are vulnerable to DoS and black hole attacks. Fortunately, there are several solutions that can be implemented in a ZRP architecture. Encryption of all traffic in a MANET using either symmetric or asymmetric encryption schemes preserve confidentiality. Deploying either an IDS within a MANET or using a fuzzy logic model to observe misbehavior of nodes can both prevent malicious nodes from affecting availability of the network. Although these solutions address relevant MANET security concerns, some of them will need to be modified to operate effectively in a tactical ZTA.

5 Mobile Ad Hoc Networks in a Tactical Zero Trust Architecture

In a tactical environment, data must flow securely and quickly within the network at the speed of relevance. A secure MANET solution must incorporate mechanisms to establish and maintain trust to align with core ZT principles. Any solution must be both agile and responsive in a chaotic network environment. By chaotic we mean that nodes are highly mobile, and appear and disappear frequently as units rapidly maneuver using vehicular or airborne means. Also, units that find themselves co-located for extended periods of time may require nodes to rapidly scale up and down [39]. Proximity to adversarial forces make MANETs at the tactical edge vulnerable to DoS-type attacks or impersonation. Adversarial and friendly electronic warfare capabilities can disrupt communication pathways. Therefore, MANETs at the tactical edge must have a robust and resilient method of evaluating and maintaining trust in the face of such operating environments.

The paradox of developing a MANET compatible with a ZTA is the infrastructure-less nature of a MANET. There are no centralized components in a MANET that ZT components such as a Policy Engine (PE), Policy Administrator (PA), or Policy Enforcement Point (PEP) can reside in. Instead of relying on a central security architecture, each node will need to implement its own PE, PA, and PEP. MANETs already decentralize trust evaluations by making each node calculate trust for their targets [40]. This approach is similar to the Pretty Good Privacy (PGP) model used for public key certification [41]. Consequently, this paper proposes the following requirements for every tactical ZTA MANET node. Maintaining these functions within each node allows each node to satisfy the core ZT principles: assume that all traffic is untrusted, enforce granular access control, and inspect and log all network traffic data. This would result in the following:

- Node Policy Engine (NPE) – responsible for evaluating trust of neighbor nodes, inspecting and logging data packets.
- Node Policy Administrator (NPA) – responsible for managing the working set of policies that can adjust to varying levels of trust inherent to the packet.
- Node Policy Enforcement Point (NPEP) – responsible for forwarding packet metadata and sending to the PE. Packets are either forwarded or dropped in the PEP based on PA rules.

An NPE functions much like a zone-based intrusion detection system (ZBIDS). Trust evaluations would be processed within the NPE for all packets transiting into or through the node, under the assumption that all network traffic is untrusted. These evaluations would not be limited to parameters used in ZBIDS, but the NPE should incorporate a wide variety of trust factors to determine a comprehensive trust score for each node. Potential trust evaluation methods could range from blockchain mining [42] to game theory to promote cooperative behavior between nodes on the network by rewarding packet forwarding [43]. These techniques have the potential to limit the network's vulnerabilities to DoS attacks. Applying these methods may lead to higher levels of confidentiality within the MANET.

Another important consideration is the rekeying of symmetric keys on the network. A compromised node that falls into adversarial hands could allow the adversary to impersonate a legitimate node. The NPE should maintain local logs of all packets sent or received. These logs should be transferred to an enterprise information and event management (SIEM) tool, which can inspect logs to further inform threat intelligence. The ZBIDS knowledge base would reside within a NPA. This knowledge base would augment the working set of routes available to the node with a set of rules based on trust scores of neighboring nodes. This working set of rules implements a granular level of access control within MANET routing. The NPEP will sit right on the node's interfaces and will forward or drop packets based on rules derived from the NPA.

Despite the paradoxical relationship between ZTA and MANET, this paper proposes requirements that implement ZT principles within a MANET. Nodes perform the trust computations for authentication, enforce access control, and log traffic data. We suggest that the existing ZBIDS security model is a suitable candidate for implementing ZTA in a MANET.

6 Conclusions

MANETs are an indispensable capability in information-age warfare because they provide a robust, self-configuring, self-healing, and resilient network to support command and control functions at the forward edge of military operations. These dynamic networks provide commanders with the ability to communicate and coordinate with geographically dispersed forces spread over a wide area. These networks are also responsive by being aboe to cope with a dynamic network topology and resilient because they are permanent infrastructure-less. These capabilities synergize with ZTA capabilities, enhancing the overall effectiveness of the network. However, the current DOD strategy for ZTAs does not provide guidance for incorporating MANETs at the tactical edge [17]. The tactical significance of scalability and performance motivated this research to identify secure hybrid routing protocols that could serve as the foundation for MANETs at the tactical edge in a ZTA.

While the paradoxical relationship between ZTAs and infrastructure-less MANETs may suggest incompatibility, we feel that they necessitate a reformulation of ZT components into MANET nodes. To that end, this paper has proposed a set of ZTA requirements that could be satisfied within the nodes of a MANET. Each of the ZTA logical components are mirrored within each node of the MANET, adhering to ZT principles as routes are discovered and maintained. Augmentation of the ZBIDS model to complement the proposed framework should be further researched, and ultimately implemented to determine communication overhead and resource consumption implications. Additional research into incorporating either game theory or blockchain mining to promote cooperation in a MANET may determine

feasibility of such trust schemes in a ZTA. Finally, development of a comprehensive NPE model that consolidates protocol-agnostic trust evaluations would identify minimum computational processing requirements for each node within the MANET.

References

[1] S. Giordano, "Mobile Ad Hoc Networks," in Handbook of Wireless Networks and Mobile Computing, John Wiley & Sons, Ltd, 2002, pp. 325–346. doi: 10.1002/0471224561.ch15.

[2] "Information Assurance Technical Framework (IATF). Release 3.1.," National Security Agency/Central Security Service, Fort George G. Meade, MD., ADA606355, 2002. Accessed: Jun. 05, 2023. [Online]. Available: https://ntrl.ntis.gov/NTRL/dashboard/searchResults/titleDetail/ADA606355.xhtml

[3] J. Kindervag and S. Balaouras, "No more chewy centers: Introducing the zero trust model of information security," Forrester Res., vol. 3, 2010.

[4] H. Ling-Fang, "The Firewall Technology Study of Network Perimeter Security," in 2012 IEEE Asia-Pacific Services Computing Conference, Dec. 2012, pp. 410–413. doi: 10.1109/APSCC.2012.23.

[5] "Single Sign On Concepts and Protocols | SANS Institute." https://www.sans.org/white-papers/1352/ (accessed Nov. 30, 2022).

[6] S. W. Shah and S. S. Kanhere, "Recent Trends in User Authentication – A Survey," IEEE Access, vol. 7, pp. 112505–112519, 2019, doi: 10.1109/ACCESS.2019. 2932400.

[7] H. Alamleh and A. A. S. AlQahtani, "Architecture for Continuous Authentication in Location-Based Services," in 2020 International Conference on Innovation and Intelligence for Informatics, Computing and Technologies (3ICT), Dec. 2020, pp. 1–4. doi: 10.1109/3ICT51146.2020.9311972.

[8] "Scalable Behavioral Authentication | IEEE Journals & Magazine | IEEE Xplore." https://ieeexplore.ieee.org/abstract/document/9378532 (accessed Dec. 01, 2022).

[9] M. Abuhamad, A. Abusnaina, D. Nyang, and D. Mohaisen, "Sensor-Based Continuous Authentication of Smartphones' Users Using Behavioral Biometrics: A Contemporary Survey," IEEE Internet Things J., vol. 8, no. 1, pp. 65–84, Jan. 2021, doi: 10.1109/JIOT.2020.3020076.

[10] "Gait-Based Continuous Authentication Using a Novel Sensor Compensation Algorithm and Geometric Features Extracted From Wearable Sensors | IEEE Journals & Magazine | IEEE Xplore." https://ieeexplore.ieee.org/abstract/document/9947076 (accessed Nov. 30, 2022).

[11] "LCDA: Lightweight Continuous Device-to-Device Authentication for a Zero Trust Architecture (ZTA) | Elsevier Enhanced Reader." https://reader.elsevier.com/reader/sd/pii/S0167404821001759?token=304E2E422568C05859BFA3119A24E3CA0FEA3395925162B59A2533927DFDD22619E8DF50C6D539216A1A8FBB885E45D8&originRegion=us-east-1&originCreation=20221102160749 (accessed Nov. 02, 2022).

[12] S. Alshomrani and S. Li, "PUFDCA: A Zero-trust based IoT device continuous authentication protocol," Wirel. Commun. Mob. Comput., 2022, Accessed: Nov. 21, 2022. [Online]. Available: https://orca.cardiff.ac.uk/id/ eprint/153958/

[13] A. Al Abdulwahid, N. Clarke, I. Stengel, S. Furnell, and C. Reich, "Continuous and transparent multimodal authentication: reviewing the state of the art," Clust. Comput., vol. 19, no. 1, pp. 455–474, Mar. 2016, doi: 10.1007/s10586-015-0510-4.

[14] B. Yu, C. Yang, and J. Ma, "Continuous Authentication for the Internet of Things Using Channel State Information," presented at the 2019 IEEE Global Communications Conference(GLOBECOM), 2019, pp. 1–6.

[15] D. Eidle, S. Y. Ni, C. DeCusatis, and A. Sager, "Autonomic security for zero trust networks," in 2017 IEEE 8th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference (UEMCON), Oct. 2017, pp. 288–293. doi: 10.1109/UEMCON.2017.8249053.

[16] D. Appelt, C. D. Nguyen, A. Panichella, and L. C. Briand, "A Machine-Learning-Driven Evolutionary Approach for Testing Web Application Firewalls," IEEE Trans. Reliab., vol. 67, no. 3, pp. 733–757, Sep. 2018, doi: 10.1109/TR.2018.2805763.

[17] DoD CIO Zero Trust Portfolio Managment Office, "DoD Zero Trust Strategy," Washington, DC, USA, Nov. 2022. [Online]. Available: https://dodcio.defense.gov/Portals/0/Documents/Library/DoD-ZTStrategy.pdf

[18] Defense Information Systems Agency (DISA) and National Security Agency (NSA) Zero Trust Engineering Team, "DoD Zero Trust Reference Architecture," Washington, DC, USA, Jul. 2022. [Online]. Available: https://dodcio.defense.gov/Portals/0/Documents/Library/(U)ZT_RA_v2.0(U)_Sep22.pdf

[19] G. Køien, "Zero-Trust Principles for Legacy Components," Wirel. Pers. Commun., vol. 121, pp. 1–18, Nov. 2021, doi: 10.1007/s11277-021-09055-1.

[20] Mahalakshmi. G, E. Uma, B. Senthilnayaki, A. Devi, C. Rajeswary, and P. Dharanyadevi, "Trust Score Evaluation Scheme for Secure Routing in VANET," in 2021 IEEE International Conference on Mobile Networks and Wireless Communications (ICMNWC), Dec. 2021, pp. 1–6. doi: 10.1109/ICMNWC52512. 2021.9688475.

[21] "(PDF) An Efficient Routing Protocol for Wireless Networks." https://www.researchgate.net/publication /2598243_An_Efficient_Routing_Protocol_for_Wireless_Networks (accessed Jun. 09, 2023).

[22] "Highly dynamic Destination-Sequenced Distance-Vector routing (DSDV) for mobile computers | Proceedings of the conference on Communications architectures, protocols and applications." https://dl.acm.org/doi/10.1145/190314.190336 (accessed Jun. 09, 2023).

[23] E. M. Royer and C.-K. Toh, "A review of current routing protocols for ad hoc mobile wireless networks," IEEE Pers. Commun., vol. 6, no. 2, pp. 46–55, Apr. 1999, doi: 10.1109/98.760423.

[24] "Ad-hoc on-demand distance vector routing | IEEE Conference Publication | IEEE Xplore." https://ieeexplore.ieee.org/document/749281 (accessed Jun. 09, 2023).

[25] D. B. Johnson and D. A. Maltz, "Dynamic Source Routing in Ad Hoc Wireless Networks," in Mobile Computing, T. Imielinski and H. F. Korth, Eds., in The Kluwer International Series in Engineering and Computer Science. Boston, MA: Springer US, 1996, pp. 153–181. doi: 10.1007/978-0-585-29603-6_5.

[26] D. Kumar, A. Srivastava, and S. C. Gupta, "Performance comparison of pro-active and reactive routing protocols for MANET," in 2012 International Conference on Computing, Communication and Applications, Feb. 2012, pp. 1–4. doi: 10.1109/ICCCA.2012.6179226.

[27] Z. Haas, M. R. Pearlman, and P. Samar, "The Zone Routing Protocol (ZRP) for Ad Hoc Networks," Internet Engineering Task Force, Internet Draft draft-ietf-manet-zone-zrp-04, Aug. 2002. Accessed: Jun. 09, 2023. [Online]. Available: https://datatracker.ietf.org/doc/draft-ietf-manet-zone-zrp

[28] Y. Kumar, Isha, and A. Malik, "Performance Analysis of Hybrid routing protocol," in 2021 2nd International Conference on Intelligent Engineering and Management (ICIEM), Apr. 2021, pp. 400–405. doi: 10.1109/ICIEM51511.2021.9445324.

[29] R. K. Singh and P. Nand, "Literature review of routing attacks in MANET," in 2016 International Conference on Computing, Communication and Automation (ICCCA), Apr. 2016, pp. 525–530. doi: 10.1109/CCAA. 2016.7813776.

[30] N. Alsafwani, M. A. M. Ali, and N. M. Tahir, "Performance Evaluation of the Mobile Ad Hoc Network (MANET) for Eavesdropping Attacks by QualN et Simulator," in 2021 IEEE 11th International Conference on System Engineering and Technology (ICSET), Nov. 2021, pp. 31–35. doi: 10.1109/ICSET53708.2021. 9612556.

[31] D. Glynos, P. Kotzanikolaou, and C. Douligeris, "Preventing impersonation attacks in MANET with multi-factor authentication," in Third International Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks (WiOpt'05), Apr. 2005, pp. 59–64. doi: 10.1109/WIOPT.2005.42.

[32] S. S. Rajput and M. C. Trivedi, "Securing Zone Routing Protocol in MANET Using Authentication Technique," in 2014 International Conference on Computational Intelligence and Communication Networks, Nov. 2014, pp. 872–877. doi: 10.1109/CICN.2014.184.

[33] B. A. S. R. Devi, J. V. R. Murthy, and G. Narasimha, "Secure zone based routing protocol for mobile adhoc networks," in 2013 International Mutli-Conference on Automation, Computing, Communication, Control and Compressed Sensing (iMac4s), Mar. 2013, pp. 839–846. doi: 10.1109/iMac4s.2013.6526523.

[34] D. Ravilla and C. S. R. Putta, "Performance of secured zone routing protocol due to the effect of malicious nodes in MANETs," in 2013 Fourth International Conference on Computing, Communications and Networking Technologies (ICCCNT), Jul. 2013, pp. 1–8. doi: 10.1109/ICCCNT.2013.6726751.

[35] I. Oakley, "Solutions to Black Hole Attacks in MANETs," in 2020 12th International Symposium on Communication Systems, Networks and Digital Signal Processing (CSNDSP), Jul. 2020, pp. 1–6. doi: 10.1109/CSNDSP49049.2020.9249524.

[36] N. Soms, R. Saji Priya, A. Sukkiriya Banu, and P. Malathi, "A comprehensive performance analysis of zone based Intrusion Detection System in mobile ad hoc networks," in 2015 3rd International Conference on Signal Processing, Communication and Networking (ICSCN), Mar. 2015, pp. 1–8. doi: 10.1109/ICSCN.2015.7219887.

[37] E. M. Shakshuki, N. Kang, and T. R. Sheltami, "EAACK—A Secure Intrusion-Detection System for MANETs," IEEE Trans. Ind. Electron., vol. 60, no. 3, pp. 1089–1098, Mar. 2013, doi: 10.1109/TIE.2012.2196010.

[38] S. Sharma, A. Jain, and N. Gupta, "Modified ZRP to Identify Cooperative Attacks," in 2016 Second International Conference on Computational Intelligence & Communication Technology (CICT), Feb. 2016, pp. 302–307. doi: 10.1109/CICT.2016.66.

[39] M. Salmanian, J. D. Brown, S. Watson, R. Song, H. Tang, and D. Simmelink, “An architecture for secure interoperability between coalition tactical MANETs,” in MILCOM 2015 - 2015 IEEE Military Communications Conference, Oct. 2015, pp. 37–42. doi: 10.1109/MILCOM.2015.7357415.

[40] G. Theodorakopoulos and J. S. Baras, “On trust models and trust evaluation metrics for ad hoc networks,” IEEE J. Sel. Areas Commun., vol. 24, no. 2, pp. 318–328, Feb. 2006, doi: 10.1109/JSAC.2005.861390.

[41] The official PGP user’s guide: | Guide books.” https://dl.acm.org/doi/10.5555/202735 (accessed Jun. 11, 2023).

[42] P. P. C. Peiris, C. Rajapakse, and B. Jayawardena, “Blockchain-based distributed reputation model for ensuring trust in mobile adhoc networks,” in 2020 International Research Conference on Smart Computing and Systems Engineering (SCSE), Sep. 2020, pp. 51–56. doi: 10.1109/SCSE49731.2020.9312998.

[43] B. U. I. Khan, F. Anwar, R. F. Olanrewaju, B. R. Pampori, and R. N. Mir, “A Game Theory-Based Strategic Approach to Ensure Reliable Data Transmission With Optimized Network Operations in Futuristic Mobile Adhoc Networks,” IEEE Access, vol. 8, pp. 124097–124109, 2020, doi: 10.1109/ACCESS.2020.3006043.