Data Packet Trust Details and Extend the Current Version

Felipe Trinidad, Kieran Scanlon, Delray Frierson, Armando Flores Munos

I. Problem Background

The contribution of this paper is to find a few ways that data packet trust is implemented in certain frameworks. There are many different frameworks to ensure the safe travel of data over nodes. We will discuss the ways that these solutions handle data packet trust. As well as any way that they can be improved in its current form. The topics that have been chosen are improvements via AI, embedded IDS/IPS solutions, a trust based model using intelligent agents and Game theory frameworks.

II. Potential Solutions

One solution that has promising results is the project that is dubbed HERMES. It is proposed by researchers at the Department of Electrical and computer engineering. Specifically for MANETS architecture this technology seeks to improve the way that trustworthiness is determined in an environment where multihop routes to the destination can have a malicious source that can hijack the packets. Hermes as they describe it assigns a determinate trustworthiness metric to the nodes based on the actions of those nodes. The Hermes framework uses a semi ring approach for its trustworthiness evaluation.This is formed from a multitude of data points first of which is an observation which must be accumulated. Which is done by the use of beta distribution, the researchers in [3] prefer the bayesian framework to accomplish this. It separates the values of trust at sampling time. Observations that have been collected prior for each router point. It calculates the probability density function based on these values and inputs these values in Bayes theorem to retrieve the packets forwarded successfully and the total number of packets. All culminate to produce the beta distribution of the system which gives the initiating values that the system needs for a router's behavior. It should be noted that this method is a purely binary value, split between trusted and non-trustworthy. The determination in between those two values is deterministic on a probability density function and the standard deviation of the confidence and trust values. For more information on the computation for these values [3] should be consulted. These two values are then combined to create the trustworthiness criteria. This only works however in an environment where a router or node is in direct contact with one another. In cases where propagation over many different nodes is necessary for a data packet to reach its destination another value is needed. Dubbed the opinion value, this metric is able to assess the trustworthiness of another router through the trustworthiness value from another router. This could however invite some problems that the paper doesn't address that could be room for improvement. One which we will return to later. A counter is also implemented to determine if a packet was forwarded successfully. This is more geared to prevent malicious activity and makes sure that the packet was actually forwarded by the node that it is linked to. In some routing algorithms Data packets use this trust in the header information which has the hops necessary to reach its destination. Unfortunately Hermes mainly determines the trustworthiness more accurately in source routing scenarios. In distance routing scenarios a packet sent downstream cannot confirm whether or not a packet was forwarded or not. This can be a problem in terms of verification because an attacker could have a malicious router and misappropriate the packet. Could lead to spoofing a false opinion value to over inflate a malicious node's trustworthiness value. This would require a packet injection technique, one that Hermes is particularly vulnerable to. A solution that I propose is to implement what [12] does in the form of a hybrid defense using game theory, specifically the Baesian game since it correlates with the theory that Hermes uses for its beta distribution. It acts as a kind of checks and balances identifying the malicious nodes by using dummy packets to track the dropping of packets. Using this in tandem with the trustworthiness method. Malicious nodes can be identified and excluded from the network. [12] furthermore recommends the use of blockchain technology as a use for the pre detection phase to increase the efficacy of this method.

III. AI as a Solutions

One of the many problems when dealing with data packet trusts is that we need to verify the integrity of the packets being sent in order to prevent any malicious attacks from being sent over to another user. While we have methods of verifying these packets, that does not mean that these methods are guaranteed to stop all malicious packets. So the question becomes how do we improve our ability to detect these hostile packets and extend the current version of packet trusts we already have in place? One solution is to incorporate AI in both the authentication process and the encryption of the data packets being sent over.

The use of AI is growing at a near-breakneck speed, and its implementation in the computing world is inevitable. Instead of trying to stop AI from being used, we should find ways to incorporate it in already pre existing networks. With AI, we can increase the security of our authentication process and lower the chances of data packets being misidentified as malicious packets. We could also use AI to learn how malicious packets adapt over time in an attempt to get around the AI protocols. The best way to describe the processes is through a feedback loop. The more data the AI is given, the better it can distinguish the differences between a legitimate packet and a malicious one. With this process, AI is able to secure the networking node it's deployed on while authenticating all traffic that goes through the node. However, that is only part of what AI can do to authenticate data packets, as it can also monitor the traffic pattern being sent through the node in real-time.

With AI-enhanced threat detection, we are able to monitor the behavior and watch the traffic patterns for any suspicious activity that may be occurring at the networking node. If the threat detection finds any suspicious activity, it can then revoke the access that data packet has been given while notifying the host of the suspicious activity within seconds. Suppose the suspicious activity turns out to be malicious. In that case, the AI can then theoretically trace where that data packet came from and block the IP address at its source, preventing the malicious packets from being sent again. However, this is all done through authentication; AI can also be used for encryption purposes as well.

Encryption makes data packets much more challenging to analyze, even with deep packet inspection(DPI) software scanning the packets for a malicious threat. However, we can view and collect the data we can see with AI, such as packet headers, traffic volume, flow data, and unencrypted handshake data. Using the data the AI has gathered, we can culminate all of that into encrypted traffic intelligence(ETI) and determine the identification of the data packet being sent. With the collected data from the ETI, we can learn the protocol being used, the application, and the service of the encrypted data packet. Now, if we combine the ETI and DPI, we increase our ability to detect malicious data packets and prevent them from being sent through the networking node. This combination of ETI and DPI will extend the current version of data packet trusts and add another layer of security and analysis to the networking node, making it safer to use.

Overall, AI can be implemented in almost anything we can think of regarding technology. Through authentication, we can create a learning feedback loop for the AI to learn and adapt to the ever-changing landscape of networking data packets. Through encryptions, we are able to use visible data gained through the packet in order to understand what those packets are potentially sending without having to decrypt the packet. Together with both authentication and encryption, a massive improvement can be found, tested, and then implemented in networking nodes. The use of AI data packet trusts can significantly improve the security of data packets, allowing the current version to be extended for a couple more years.

IV. IDS/IPS In Data Packets

One solution to improving the security of data packets is the implementation of intrusion detection systems and intrusion prevention systems directly on the packets. An IDS is a hardware or software function that gathers and analyzes data from different areas within a network to identify a possible security attack. After a potential threat is detected, it will sound an alarm. Intrusion prevention is an action that is taken after the IDS alerts a potential breach. There are different approaches to intrusion detection. One of many factors is placement. Typically, they can be found at strategic points within a network to monitor packets moving in and out. They can also be placed on IoT devices with network access.

IDS and IPS primarily use two different methods to analyze sensor data: anomaly detection and signature detection. Anomaly detection observes the typical behavior of different users to determine if they are legitimate or not. If a user's actions are outside of data that is considered normal, the IDS will sound an alarm. It involves the collection of data relating to the behavior of legitimate users over a period of time. Signature detection uses a set of known malicious data patterns or attack rules and compares them with current behavior. It can only identify known attacks that have been previously attempted.

As of right now, there are several issues that stem from implementing intrusion detection onto data packets. Most of them are simply because we do not yet have the processing capabilities for this approach. Data packets involve complex analysis and pattern recognition. Because there is so much variety, it would require a lot of resources and may negatively affect the host device sending out the packet. It also

would not be able to scale very well because it may overwhelm the network easily.

Many communication channels encrypt data packets while in transit, so an IDS would require them to be decrypted before being implemented into a packet. Lastly, there is the matter of updating and configuring the IDS to combat new security threats. This prevents a centralized standard for security measures. However, all of the issues listed above are only concerning implementing IDS and IPS at this time. Thanks to the rapid progression in technology, largely thanks to artificial intelligence, we have already made a countless number of breakthroughs we have previously believed to be far away.

With the track that we are on, it will only be a short time until host devices can achieve the necessary processing power to implement IDS. For this potential solution, there will be trade-offs similar to what was discussed previously. While the potential advantages are only in theory, it is worth exploring the possibilities. Implementing intrusion detection systems into data packets will allow for real-time analysis and will provide insights into network traffic. Additionally, it will be able to highlight when and where an intrusion took place immediately after it happens. Combined with machine learning and artificial intelligence, it can also automatically trace back to where the interception happened and blacklist the undesired IP address. Another potential benefit would be a significant reduction in latency when it comes to reporting information to the IDS's database. This may prove useful to various companies that utilize time-sensitive applications. Lastly, an IDS implementation would enhance user privacy. Because sensors would only detect modifications or interceptions, it will only extract relevant information to add to its database. That data will only be used to constantly improve its own security measures and will be able to more accurately stop a threat at the source.

Once again this solution is far from perfect as it cannot yet be tangibly experimented on. At this time, our commonly found devices will not be able to handle intrusion detection systems coming in and out of our respective network. For the time being, it is most efficient to place intrusion detection strategically at crucial points in the network or any host devices. We also will require current IDS/IPS systems to continue developing their database by detecting and analyzing what would be considered malicious.

As it currently stands, the current version of data packet trust can be extended because we are not yet at the point where we can implement a substantial update. Artificial intelligence points to a solution most researchers have been seeking. However, due to its nature, AI still needs time to grow and collect data. When it comes to security, there will never be a foolproof solution to preventing data breaches. AI will very likely be used in tandem with technology we currently use to give us many options to work with.

V. Trust Based Model using intelligent Agents

The network of Internet of things allows sensors and embedded systems to be at the forefront of innovation and enhance a human's ability to interact with medical equipment, physical security, automobiles, and payment processing. IoT has gained popularity as part of the Do It Yourself projects with hobbyists. Professional IoT manufacturers are using Machine to Machine, People to People, and Machine to People. Machine to machine is used throughout manufacturing plants to connect sensors through IP to enhance monitoring and machine performance analytics.The amount of IoT information is increasing hence a need for great computational processing power.

IoT devices need 802.15 wireless personal area networks for short range communication.

Within 802.15 nodes can operate in a star topology dividing the peer to peer topography into clusters which supports unicast and broadcast. Short range IoT communication objects can be used such as NFC for payment transactions. Students have often pushed for innovation and raspberry PI's. These small yet powerful computational devices have allowed students to develop biometric systems such as palm vein pattern and models to extract fingerprint and footprint of newborn babies.3-bit or 7 bit flag bits are used as attributes in IPv6 header for the use of Quality of Service. IoT devices could be used as a Black hole and with limited resources disrupt the usage of the device IPv6 and IPv4 are widely used and supported in the IoT network at the network layer of the OSI model. The Use of IPv6 possesses a greater security attribute due to its reformed header using Link-Local Addresses. Link local Addresses is a unicast address in the packet which helps with security because they can not be used outside of the link.

To diminish the amount of Denial of Service attacks and Distributed Denial of service attacks replacing broadcast messages with anycast messages would be effective.

An innovative IoT object is Sintelurs waste management which determines the filling level of various types of plastics, paper and aluminum cans using the machine to machine communication through General Packet Radio Service. Internet of things. communication strategies include device to device, device to cloud, device to gateway, and device to application. Communication types and definitions: Device to Device, Device to application, Device to Gateway, and Device to cloud. Widely used telecommunication infrastructures like 3G, 4G, and 5G connect IoT devices to cellular

broadband.Routing based communication considers routing problems such as traffic, energy consumption. packet delay and response time. A solution was proposed to countermeasure routing problems with a multihop routing method that would allow IoT device communication with minimum energy consumption. An fascinating article mentioned Authentication encryption communications. An interesting research method involved combinatorial offloading secure operations to determine energy consumption, memory saving, and data congestion. The challenge throughout all aspects of communication is upholding confidentiality, integrity, and authentication. Public key infrastructure and trusted execution environmental techniques can be proven beneficial for challenge. Allowing the Internet of Things a secure connection would require a cloud network that can handle a challenging increase in size and mobility of end users.

With Trust based Monitoring scheme middle and intelligent agents are deployed to manage communication security. Intelligence agents allow a secure connection by exchanging trust and signal strength to the middleware.
Trust based monitoring approach allows for lower response time, detection times, misdetection probabilities, and extending the longevity of a network.

Allowing the Internet of Things a secure connection would require a cloud network that can handle a challenging increase in size and mobility of end users. With Trust based Monitoring scheme middle and intelligent agents are deployed to manage communication security. Intelligence agents allow a secure connection by exchanging trust and signal strength to the middleware.
Trust based monitoring approach allows for lower response time, detection times, misdetection probabilities, and extending the longevity of a network. Smart devices connected through the internet present several challenges such as mobility, interoperability, scalability, security, and privacy. Service level authentication is essential to combat security threats. IoT devices have the ability to have network dynamics, mobility, and flexibility which should be satisfied by emerging security measures. Intrusion detection systems are used throughout this Trust based Model in wireless communication in order to monitor the behavior of the devices on the network. Intelligent agents are programs that allow functionalities such as data aggregation, analysis, and computations. Intelligent Agents as security monitors are used because of their easy interoperability and smart decision making.The design of a trust monitoring system to prevent malicious activity user access and MAC spoofing in IoT communications. IAs that learn and evaluate the behavior of the communicating devices over distinct beacons. Creating a lightweight Trust Based Model scheme for securing the internal communication of devices. The model helps to deny false data injection and flooding. This process is facilitated by elliptic curve cryptography.

References

[1] G. Eason, B. Noble, and I. N. Sneddon, “On certain integrals of Lipschitz-Hankel type involving products of Bessel functions,” Phil. Trans. Roy. Soc. London, vol. A247, pp. 529–551, April 1955. *(references)*

[2] J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68–73.

[3] Zouridaki, Charikleia, et al. “Hermes: A Quantitative Trust Establishment Framework for Reliable Data Packet Delivery in Manets.” *Journal of Computer Security*, IOS Press, 1 Jan. 2007, content.iospress.com/articles/journal-of-computer-security/jcs278.

[4] Wilber, Laura. “Four Pragmatic Ways AI Is Already Improving Zero Trust Network Access.” *The Fast Mode*, The Fast Mode, 31 July 2023, www.thefastmode.com/expert-opinion/32877-four-pragmatic-ways-ai-is-already-improving-zero-trust-network-access.

[5] Wilber, Laura. “Four Pragmatic Ways AI Is Already Improving Zero Trust Network Access.” *The Fast Mode*, The Fast Mode, 31 July 2023, www.thefastmode.com/expert-opinion/32877-four-pragmatic-ways-ai-is-already-improving-zero-trust-network-access.

[6] “How AI/ML-Based Deep Packet Inspection Tames New Age...” *Ipoque*, www.ipoque.com/blog/cryptography-with-dpi-and-eti. Accessed 11 Dec. 2023.

[7] “What Is the True Potential Impact of Artificial Intelligence on Cybersecurity?” *CSO Online*, 10 Apr. 2023, www.csoonline.com/article/574985/what-is-artificial-intelligence-s-true-potential-impact-on-cybersecurity.html.

[8] Sivagaminathan, Vaishnavi, et al. “Intrusion Detection Systems for Wireless Sensor Networks Using Computational Intelligence Techniques.” Cybersecurity, vol. 6, no. 1, Dec. 2023. EBSCOhost, https://doi-org.avoserv2.library.fordham.edu/10.1186/s42400-023-00161-0.

[9] Saif, Sohail, et al. “MLIDS: Machine Learning Enabled Intrusion Detection System for Health Monitoring Framework Using BA-WSN.” International Journal of Wireless Information Networks, vol. 29, no. 4, Dec. 2022, pp. 491–502. EBSCOhost, https://doi-org.avoserv2.library.fordham.edu/10.1007/s10776-022-00574-7.

[10] Sanghi, A., et al. “Anomaly Detection in Data Plane Systems Using Packet Execution Paths.” SPIN 2021 - Proceedings of the 2021 ACM SIGCOMM Workshop on Secure Programmable Network

INfrastructure, Aug. 2021, pp. 9-15–15. EBSCOhost, https://doi-org.avoserv2.library.fordham.edu/10.1145/3472873.3472880.

[11] Sharma, Niharika, and Bhavna Arora. “Review of Incremental and Online Learning Methods for Network Anomaly Detection.” Turkish Online Journal of Qualitative Inquiry, vol. 12, no. 7, Aug. 2021, pp. 6367–94. EBSCOhost, search.ebscohost.com/login.aspx?direct=true&db=ehh&AN=161812005&site=eds-live.

[12] Author links open overlay panelS Vijayalakshmi a, et al. “Hybrid Defense Mechanism against Malicious Packet Dropping Attack for Manet Using Game Theory.” *Cyber Security and Applications*, Elsevier, 26 Nov. 2022, www.sciencedirect.com/science/article/pii/S277291842200011X.

[13] S. Tayeb, S. Latifi and Y. Kim, "A survey on IoT communication and computation frameworks: An industrial perspective," *2017 IEEE 7th Annual Computing and Communication Workshop and Conference (CCWC)*, Las Vegas, NV, 2017, pp. 1-6, doi: 10.1109/CCWC.2017.7868354.

[14] Sharma, Ankush. “Review on Communication Protocols Internet of Things (IoT).” (2021).

[15] Multi‐level trust‐based intelligence schema for securing of internet of things (IoT) against security threats using cryptographic authentication

---------- **********----------