Poster: Mitigating Blackhole Attack in NDNoT

Afia Anjum
Department of Computer Science and Engineering
University of Texas at Arlington
afia.anjum@uta.edu

Habeeb Olufowobi
Department of Computer Science and Engineering
University of Texas at Arlington
habeeb.olufowobi@uta.edu

***Abstract*—Named Data Networking (NDN) has emerged as a networking model to support the Internet of Things (IoT) content distribution, security, and mobility. NDN provides promising solutions through its named content, in-network caching, and named-based routing approach to overcome the constraints of the TCP/IP model. However, IoT endpoints tend to switch to sleep mode often to save energy due to their computational power and strict energy restrictions, resulting in being in stealth mode or dead address that causes dropped or silently discarded packets. In this paper, we introduce a reputation-based forwarding approach with a reactive reputation updating mechanism to address the blackhole attacks in the NDN-enabled IoT network.**

***Index Terms*—Blackhole, NDN, IoT, Forwarding Approach**

I. Introduction and Problem Statement

The Internet of Things (IoT) is revolutionizing several industries and applications with the explosive growth of heterogeneous internet-connected devices. These devices generate an onslaught of data allowing for real-time information processing and data sharing facilitated by the technological advancement in communication networks. Named Data Networking (NDN) [1], an emerging Internet communication architecture provides benefits such as efficient content access, dissemination, and security to IoT applications. The application of NDN in different IoT domains has specifications in terms of data reliability, dependability, and availability constraints. NDN-enabled IoT (NDNoT) offers several benefits to efficiently delivering content in a high mobility network with its unique characteristics of content naming, in-network caching, and content-centric security.

Despite the benefits, NDNoT has several challenges, including storage constraints, signature verification overhead, and security vulnerabilities for caching data in the network. Moreover, when employed as an IoT communication protocol, NDN inherits the attributes of resource constraint IoT nodes such as memory, CPU, and power limitations. Storage constraints make it difficult for NDN to store content in each router of the data transmission path, and limited CPUs impose computational complexity when validating a signature. Also, to minimize energy consumption and battery life constraints of IoT nodes, sleep cycle timing behavior has been introduced for battery-powered IoT nodes that place the nodes in sleep, sense, and connect mode when necessary to execute their tasks.Furthermore, reduced messaging for short data transactions and simplified monitoring of neighbor cells have been proposed to extend the battery life. However, in NDNoT communication, data is transmitted from the nearest node cache, and the nodes between the data consumer and provider need to participate in forwarding the request and the data packet. Consequently, an IoT node that is the next logical stop for data routes that go to sleep mode during communication may cause a packet drop or dead address in the network, referred to as a blackhole attack, as shown in Figure 1. Each node that receives the data contributes to the routing process, and IoT nodes with considerable battery power can silently drop packets by going to sleep mode, executing the blackhole attack at the network layer.

Although a blackhole attack is structurally easy to achieve, the attack can be stealthy and remain unnoticed as the attacking nodes only drop packets. Prior works have proposed different approaches to address this attack, research specific to the NDNoT environment is very limited [2], [3]. Therefore, our goal in this paper is to address the blackhole attack in the NDNoT environment executed by IoT nodes that constantly enters sleep mode during the data routing while having considerable battery power. We propose a reputation-based technique that encourages IoT nodes to stay awake during the routing process to mitigate blackhole attacks. Using the device's battery power, we proposed a reactive reputation updating mechanism to assign reputations and then determine a new stature upon the performance of the nodes during the routing process.

II. Related Works and Limitations

Prior works have proposed different solutions for blackhole attacks in the NDN-IoT environment [2]–[6]. Mick et al. [4] propose a secure routing solution to protect the network using a lightweight authentication mechanism. DiBenedetto et al. [5] address the data packet drop issue originating from poisoned content using consumer feedback. Based on the consumer report, the route that delivered the poisoned data is considered the least desired choice for future interests. Lei et al. [6] provide a probabilistic forwarding technique that evaluates interface availability and selects the next hop during packet forwarding by taking into account different network attributes such as packet loss and delays. Zhu et al. [2] propose a blockchain-based network model and state the need for a motivation policy to solve blackhole attacks in the NDN-IoT environment. However, blockchain would incur additional overhead for recording all requesting and forwarding information, including the hash of interest/data packets. Yang and Chen [3] propose SmartDetour, a

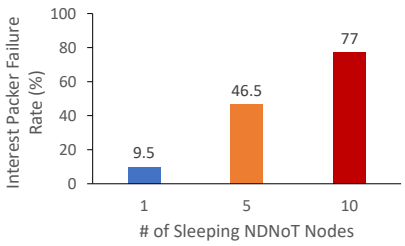

Fig. 1: Interest packet drop rate increases with the increase in sleeping nodes

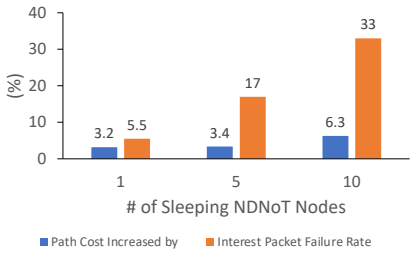

Fig. 2: Avoiding sleeping nodes increases route costs, and the packet drop issue persists

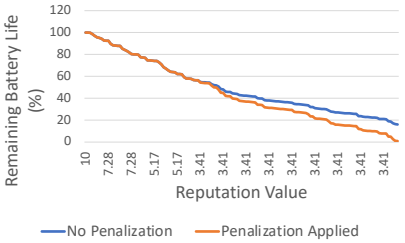

Fig. 3: Experimental result of reputation-based forwarding approach: Here, the battery is draining more power when the reputation is less than threshold.

reputation-based probabilistic forwarding technique to address blackhole attacks in the NDN-IoT environment. Unlike [5], which avoids the entire path that created the blackhole, the authors identify and then sidestep the attacker node.

NDN employs the best-route strategy to forward interest with the minimal routing cost [7]. The approaches described above address the blackhole attack by avoiding the route or node causing the packet loss. Avoiding any node in that route causes the interest packet to traverse using another path, thereby incurring additional costs and a delay in data delivery, as depicted in Figure 2. Moreover, avoiding the identified attacking node is ineffective in addressing packet drops created by sleeping IoT nodes, as a drop in interest packet can occur if only the sleeping node has the requested information or if there is no other path from the source to the destination. Furthermore, since IoT nodes operate in a collaborative system, a node may discard packets selfishly to save energy when realizing that the forwarding path will always be avoided if detected.

III. Proposed Forwarding Approach

We proposed a neighbor rating-based forwarding method. In addition to the current interest and data packets in NDN architecture [1], we propose a new packet called a *sleep packet* and introduce three new fields associated with each interface in the NDN router's FIB table; status $S \in \{awake, sleep\}$, remaining battery life, $RBL \in [0\%, 100\%]$, and reputation value, $RV \in [0, 10]$. This approach encourages nodes to be active and conserve energy only when necessary. When a node needs to switch to sleep mode to save energy, it will notify its neighbors using the sleep packet, adding the remaining battery power. Upon the arrival of the sleep packet, the neighbors will compute the node's reputation value using $RV = RV - e^{\theta}$. Here e is the exponential constant and θ is the penalization factor ($\theta = RBL$). The RV is only calculated when $RBL > 40\%$ to make a trade-off between keeping the nodes awake and preserving energy when necessary. This condition made the RV in Figure 3 constant at 3.41. Each neighboring node will update the S, RBL, and RV fields of their router's FIB for the interface that switched to sleep mode.

Based on the node reputations, we propose a forwarding approach and a reactive reputation updating mechanism that update the reputation value based on the path cost with and without the sleeping node. In addition, to penalize the nodes with an $RV < 5$, an additional delay $D = 10 - RV$ is applied when transmitting data to that node. Also, since nodes with a low reputation must wait longer for data and $RBL \propto \frac{1}{active\ time}$, nodes who switch to sleep mode frequently will lose more energy due to penalization, as depicted in Figure 3. If the cost of the most cost-effective path containing a sleeping node s is the same as the cost of the subsequent path taken to avoid node s, RV of s (RV_s) will be reversed. Here, $RV_s = RV_s + e^{-\gamma}$, where $\gamma \in [0, 10]$ and $\gamma \propto RBL$. Consequently, the sooner the nodes realize that continuously switching to sleep mode to drop packets while having sufficient energy drains more battery power, the longer they stay awake.

IV. Conclusion

We have proposed a reputation-based forwarding approach using reactive reputation updating to mitigate blackhole attacks in an NDNoT environment. This approach encourages battery-powered constrained IoT nodes to stay active and minimize sleep cycles to participate in the data delivery process in the collaborative network. Future work concerns the consideration of malicious nodes in the network, such as a node going to sleep mode without sending a sleep packet.

References

[1] L. Zhang, A. Afanasyev, J. Burke, V. Jacobson, K. Claffy, P. Crowley, C. Papadopoulos, L. Wang, and B. Zhang, "Named data networking," *ACM SIGCOMM Computer Communication Review*, vol. 44, no. 3, 2014.

[2] K. Zhu, Z. Chen, W. Yan, and L. Zhang, "Security attacks in named data networking of things and a blockchain solution," *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 4733–4741, 2018.

[3] N. Yang, K. Chen, and M. Wang, "Smartdetour: Defending blackhole and content poisoning attacks in iot ndn networks," *IEEE Internet of Things Journal*, vol. 8, no. 15, pp. 12 119–12 136, 2021.

[4] T. Mick, R. Tourani, and S. Misra, "Laser: Lightweight authentication and secured routing for ndn iot in smart cities," *IEEE Internet of Things Journal*, vol. 5, no. 2, pp. 755–764, 2017.

[5] S. DiBenedetto and C. Papadopoulos, "Mitigating poisoned content with forwarding strategy," in *2016 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*. IEEE, 2016, pp. 164–169.

[6] K. Lei, J. Yuan, and J. Wang, "Mdpf: An ndn probabilistic forwarding strategy based on maximizing deviation method," in *2015 IEEE global communications conference (GLOBECOM)*. IEEE, 2015, pp. 1–7.

[7] M. Z. Ahmed, A. H. A. Hashim, A. M. Hassan, O. O. Khalifa, A. H. Alkali, and A. M. Ahmed, "Performance evaluation of best route and broadcast strategy for ndn producer's mobility," *International Journal of Engineering and Advanced Technology (IJEAT) ISSN*, 2019.