April 2023

INTELLIGENT INTENT-RECOMMENDER IN INTENT-BASED NETWORKING (IBN) USING UNKNOWN TRAFFIC IDENTIFICATION

Claire Y. Chour

Doosan Jung

Qihong Shao

Dave Zacks

INTELLIGENT INTENT-RECOMMENDER IN INTENT-BASED NETWORKING (IBN) USING UNKNOWN TRAFFIC IDENTIFICATION

AUTHORS:
Claire Y. Chour
Doosan Jung
Qihong Shao
Dave Zacks

ABSTRACT

An intent recommendation system for an Intent-Based Networking (IBN) system classifies unknown traffic in a network environment using machine learning. The intent recommendation system provides a network administrator with full visibility of their network traffic so they can properly define their intent for network traffic flows within a traditional IBN model. Based on the categorization of unknown network traffic the intent recommendation system provides recommendations for how the network administrator should define their intents for each unknown network flow. The network administrator may choose whether or not to follow the intent recommendation for each unknown network traffic flow. A feedback loop incorporates the decision of the network administrator to validate and improve the suggested intents for each unknown network traffic flow cluster.

DETAILED DESCRIPTION

Network administrators typically track the major applications of traffic flowing through their network, but may be surprised to see network traffic that is not associated with a known application flowing through their network. For instance, users that use a Virtual Private Network (VPN) may use the network for encrypted traffic with no insight into the application generating the network traffic. These unknown and encrypted traffic flows, which may be unknown to the network administrators, may be dangerous or benign. Additionally, a lack of awareness of all types of traffic flows may lead to issues for the network, such as operational inefficiencies, higher risk, data loss, and/or leaks. These issues may raise compliance issues since they increase the likelihood of uncontrolled data flows. If a large volume of unknown traffic turns out to be benign and/or authorized, the network administrators must properly manage this ‘hotspot’ in the network environment.

As the network management system proposed herein becomes more familiar with specific network environments, the system begins to recognize these types of unknown traffic and suggests possibilities for including the previously unknown traffic flows in the managed traffic so that network administrators' intents are better fulfilled. Additionally, if the unknown traffic flows present dangerous and/or malicious situations, the network management system may recommend blocking the traffic flows to mitigate the damage to the network.

Intent-based networking is a software-driven process that captures an organization’s business intent, translates the business intent into network policies, and applies the network policies consistently across the network through continuous verifications, insights, and corrective actions. For instance, an organization may prioritize network traffic for specific customers, deprioritize social media network traffic, and completely block network traffic from specific countries. Intent-based networking reduces human errors and risks while improving operational efficiencies.

When network administrators typically define their intents for handling traffic flows in their managed network, they can only define intents for traffic flows that are known. However, if administrators are unaware of some of the traffic flows in their network, these unknown traffic flows may not be covered by the defined intents, which can raise several security concerns. If network administrators remain unaware of the unnoticed and uncontrolled data flow, these network flows may restrict the administrators’ ability to properly set their intents. Even if the intents are properly set for the known data traffic flows, the actual network may suffer from deteriorating performance or integrity due to the unknown traffic flows.

Typically, network traffic detection/identification may include one or more techniques that record network information such as port addresses, packet payload (e.g., Deep Packet Inspection), and flow-based measurements. The network management system described herein leverages Machine Learning (ML) techniques when classifying network traffic flows. Additionally, the network management system incorporates an intelligent IBN recommender to assist network administrators by raising awareness of unknown traffic flowing through their networks. The intelligent IBN recommender in the network management system provides recommendations on how network administrators should

define their intents. By leveraging ML models for detecting and classifying previously unknown network traffic flows, the network management system ensures that network administrators properly set their intents for the traditional IBN model.

Studying and analyzing unknown traffic patterns presents a complex challenge in modern networks. With the emerging concept of IBN, the importance of capturing and handling unknown traffic is continuously increasing. The network management system analyzing and classifying previously unknown traffic flows is important for network administrators to set their intents on traffic handling with full visibility about the network. For instance, the unknown traffic may be unsecure or risky enough that it presents a security issue for the entire network and the network administrators will want to define an intent to completely block the risky traffic flows. Alternatively, the network administrators may want to define an intent for the unknown traffic flows to monitor the traffic flow and possibly redirect the traffic flow.

Additionally, the analysis of unknown network traffic flows allows the network administrators to become aware of the potential implicit impact of intents that are based on the known network traffic flows. For instance, network administrators may define intents that are optimal for the traffic patterns of known network flows, but are suboptimal for handling the unknown network flows. Having insight into the previously unknown traffic flows may uncover information that affects the realization of the intents for the known traffic flows.

To address the issues of unknown traffic flows in a network, the techniques described in the proposal provide a network management system that intelligently provides full visibility and recommendations that enable network administrators to set fine-grained intents for known traffic flows and previously unknown traffic.

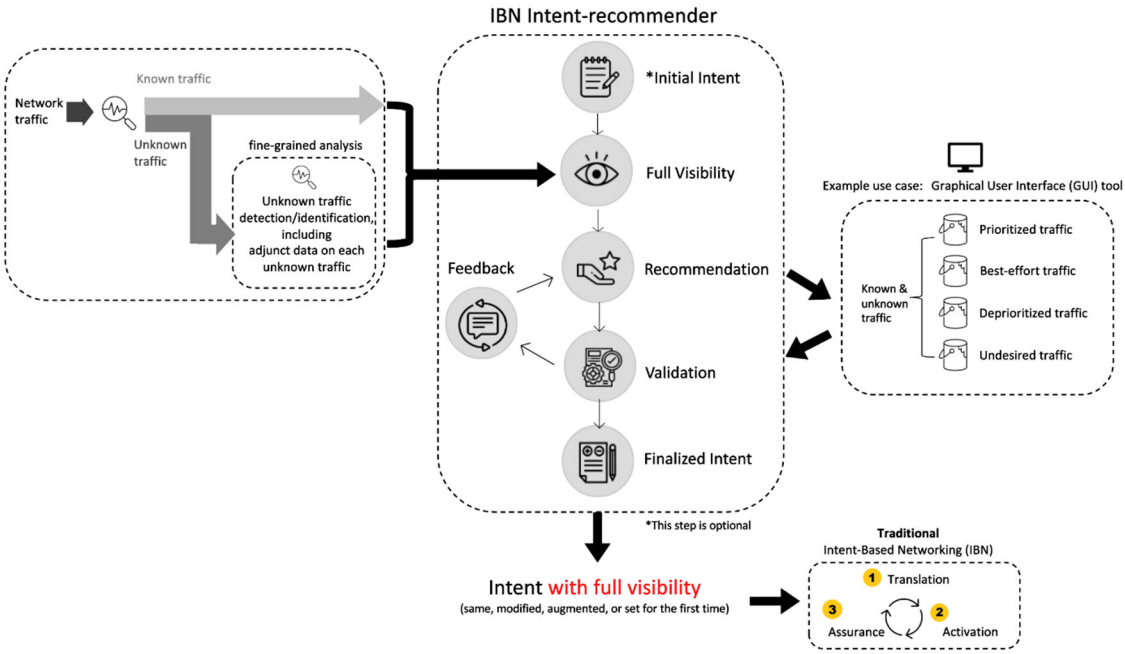

Figure 1 - High-level Overview of an IBN Intent Recommender

Figure 1 provides a high-level overview of the network management system and shows the operation of the IBN intent recommender to improve the visibility for a network administrator to generate intents for all network traffic that crosses their network. Initially, the network administrator may determine initial intents based on the known network traffic. Alternatively, the network administrator may choose to set their intents after obtaining full visibility into all of the traffic in their network. Setting intents without understanding all of the traffic in the network may lead to suboptimal outcomes causing inefficiencies in network operation and/ or security.

The network management system provides full visibility into the network traffic through the addition of unknown traffic that is found in the network environments by leveraging machine learning techniques for unknown traffic detection and fine-grained identification. The unknown traffic detection and identification producing clusters of unknown traffic for the network administrator to consider defining intents. Machine learning approaches using statistical features of network flows have been widely studied in clustering of unknown traffic. Some examples of machine learning techniques include dual-path autoencoder-based clustering, using the similarity of packets to categorize unknown traffic, and automatic K-means clustering.

Machine learning techniques may not be sufficient to identify unknown traffic by themselves. Specifically, the clustered result or the classification result may not include sufficient detail, leaving the network administrators to treat them as bulk/undefined traffic. In one example, the network management system includes adjunct data associated with the flow (e.g., source and destination subnets, Domain Name System (DNS) information, certificates, etc.) into the identifying process. By understanding adjunct and relevant information around the unknown traffic, the network administrator may determine their intents better. For instance, the adjunct data associated with an unknown traffic flow may narrow down the possible applications causing the network traffic from a wide variety of potential applications to a small handful of applications. This helps further identify what the unknown traffic is so that network administrators may differentiate between clusters of unknown traffic flows and set differentiated intents for one or more of the traffic flows.

Based on the generated clusters of unknown traffic, the network management system may recommend intents for each cluster based on machine learning techniques, as shown in the Recommendation step of Figure 1. For instance, the system management system may discover that cluster A of previously unknown traffic exhibits similar behavior to a known malicious traffic flow, leading to a recommended intent that redirects, investigates, and/or blocks the traffic in the cluster A. Alternatively, if the network management system determines that the cluster A is suspicious but not entirely malicious, then the network management system may recommend and intent to closely monitor and record the traffic flows in cluster A.

In the Validation step shown in Figure 1, after the IBN Intent-recommender's recommendation, the network administrator may decide whether to follow the recommended intent after having full visibility of all network traffic. In one example, the network management system may deploy a simple drag-and-drop Graphical User Interface (GUI) for network administrators to express their intents easily. The IBN Intent-recommender may make recommendation on how the network administrator should allocate applications to specific network flows, but the network administrator retains control over the application associated with each network flow and the intent for each application and network flow.

In the Feedback step shown in Figure 1, the IBN Intent-recommender includes a feedback loop to improve the recommendation system. The feedback loop validates that the recommended intents for traffic flows are reasonable and followed by the network administrators. If the recommendation was not followed, the network management system may investigate to determine a cause for the deviation from the recommended intent. The results from the investigation may further improve the machine learning models behind the recommendations.

After obtaining full visibility into the known and previously unknown traffic in their network, the network administrators may finalize their intents for one or more categories of network traffic. If the network administrators have previously set their intents (i.e., in the Initial Intent step of Figure 1), then the network administrators may maintain their initial intents, or they may modify or augment their initial intent based on the recommended intent from the IBN Intent-recommender. If the network administrators chose not to set initial intents for the known traffic flows, then they can set their intents for both known and previously unknown traffic flows with full visibility of the network. When these steps are completed and network administrators have set their intents, the intents may be provided to a traditional IBN, which may start a translation phase to translate the intents into actionable rules in the network elements.

Some of the benefits of incorporating the IBN Intent-recommender with unknown traffic detection/identification include:

- Maximum awareness: Raising awareness of the network data that flows across a network environment, specifically the previously unknown network traffic.
- Maximum network security: Since the IBN Intent-recommender provides full visibility of a customer's network, it can quickly detect unknown traffic and determine whether the unknown traffic may be safe or malicious.

Consider various example use cases, as follows:

Use Case #1: Following the IBN Intent-recommender's Suggestion

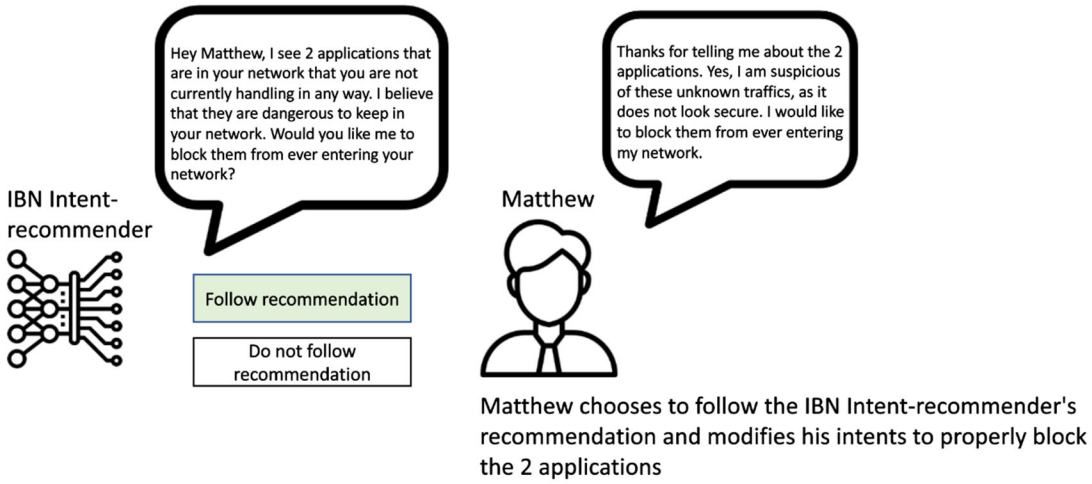

Figure 2 - Example Use Case of Following IBN Intent-recommender's Suggestion

In the use case illustrated in Figure 2, the network management system detects network traffic from unknown applications in the network environment. Matthew, a network engineer, states his intents given what he knows about the network traffic flowing through his network. Leveraging existing ML techniques, the IBN Intent-recommender identifies two different unknown applications providing network traffic in Matthew's network environment. The IBN Intent-recommender identifies one of the unknown applications as dangerous. Since this network traffic is malicious, the IBN Intent-recommender suggests that Matthew set an intent to block this traffic, as his initial intents would not have blocked this unknown traffic. Matthew must decide whether he wants to follow the IBN Intent-recommender's suggestion. As seen in Figure 2, Matthew agrees to modify his intents, and proceeds into the translation phase of IBN. Since the suggested intent of blocking the unknown traffic was followed, using a feedback loop, the IBN Intent-recommender positively reinforces the machine learning model that generated the recommendation.

Use Case #2: Not Following the IBN Intent-recommender's Suggestion

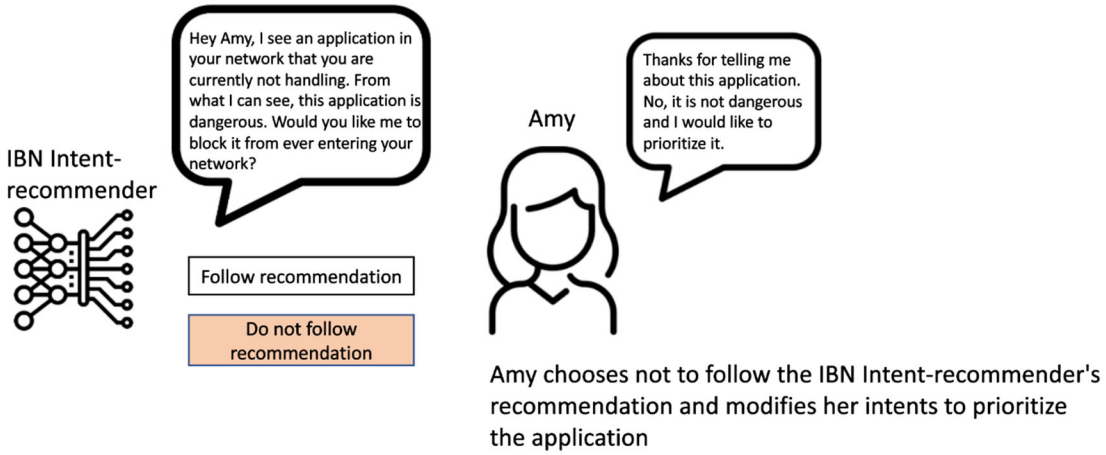

Figure 3 – Example Use Case of Not Following IBN Intent-recommender's Suggestion

In the use case shown in Figure 3, the IBN Intent-recommender detects an unknown application generating network traffic in the network environment. Leveraging existing ML techniques, the IBN Intent-recommender identifies the unknown application as malicious. The IBN Intent-recommender suggests that Amy, a network engineer for the network environment, sets an intent to block the network traffic from the previously unknown application. Amy must decide whether she wants to follow the IBN Intent-recommender's suggestion. In this example, Amy determines that the traffic from the identified application is not dangerous and may be actually necessary to include the network traffic in the network environment. Therefore, as seen in Figure 3, she does not follow the recommendation and instead sets an intent to prioritize the network traffic from the previously unknown application. Since the suggested action of blocking the unknown traffic was declined, using a feedback loop, the IBN Intent-recommender negatively reinforces the machine learning model that generated the recommendation.

Use Case #3: Drag-and-drop Graphical User Interface (GUI)

In one example, the network management system creates a Graphical User Interface (GUI), enabling network administrators and engineers to express their intents more intuitively. After the IBN Intent-recommender's suggestion, network administrators must determine whether to follow the suggestion after having full visibility of all network traffic. Even though the network administrators now have a deeper understanding of all the network traffic flowing through their network, updating multiple network elements to block or prioritize certain applications presents a challenge. The network management system may provide an easy GUI tool so that network administrators can simply drag and drop each application into predetermined sets of example intents.

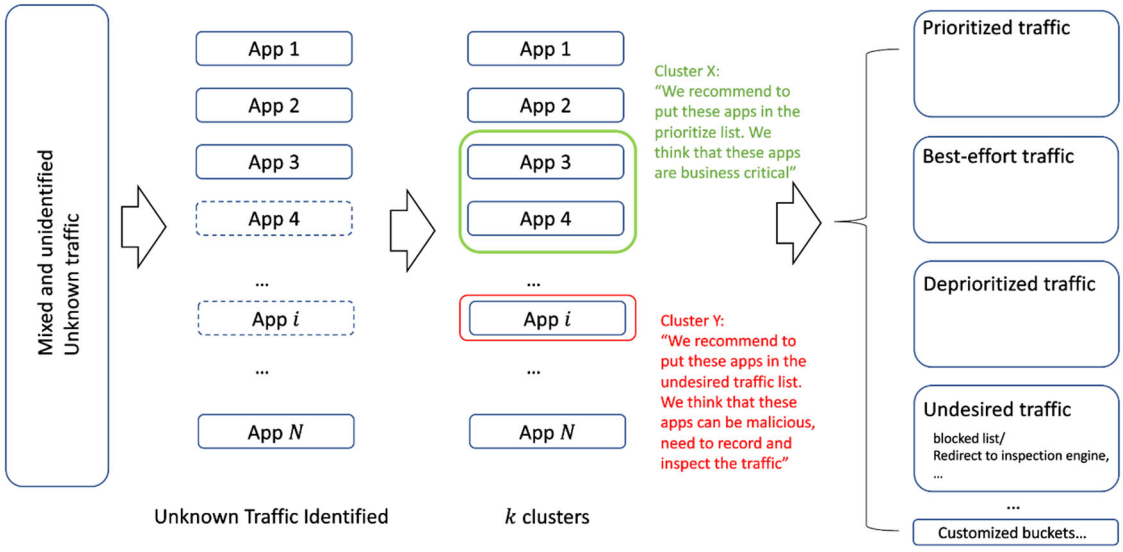

Figure 4 – Recommending Intents Based on the traffic clusters generated via ML

As an example, Figure 4 displays a set of example intents for a network administrator to assign network traffic from specific applications: prioritized, best-effort, deprioritized, and undesired traffic. Network administrators may have more granular intents. For instance, within the intent set for undesired traffic, there could be 'redirection,' 'block at any circumstances by default,' or 'further investigation.' Network administrators may define additional customized intents specific to their network situation. For instance, a network administrator may want a specific treatment for any unidentified traffic with certain properties. These granular and/or customized intents may be added, in addition to

the four example buckets shown in Figure 4, to "customized buckets". This bucket may include specific handling instructions (e.g., an extra layer of security, encryption, controller for rate limit, etc.) for network traffic assigned to this intent.

As shown in Figure 5, network administrators may express their intent with this easy drag-and-drop tool, allowing an Intent-Based Network (IBN) to translate the intent, configure the network elements, and monitor the network in an effort to realize the network administrator's intent. In the example shown in Figure 5, the network administrator dragged 'App 4' over to the 'Prioritized traffic' intent to indicate that network traffic from App 4 should be prioritized. Similarly, the network administrator dragged App i' over the 'Undesired traffic' intent to indicate that network traffic from App i should be blocked, redirected, or sent for further investigation. Any remaining applications that the network administrator does not explicitly address may be added to a default intent (e.g., Best-effort traffic).

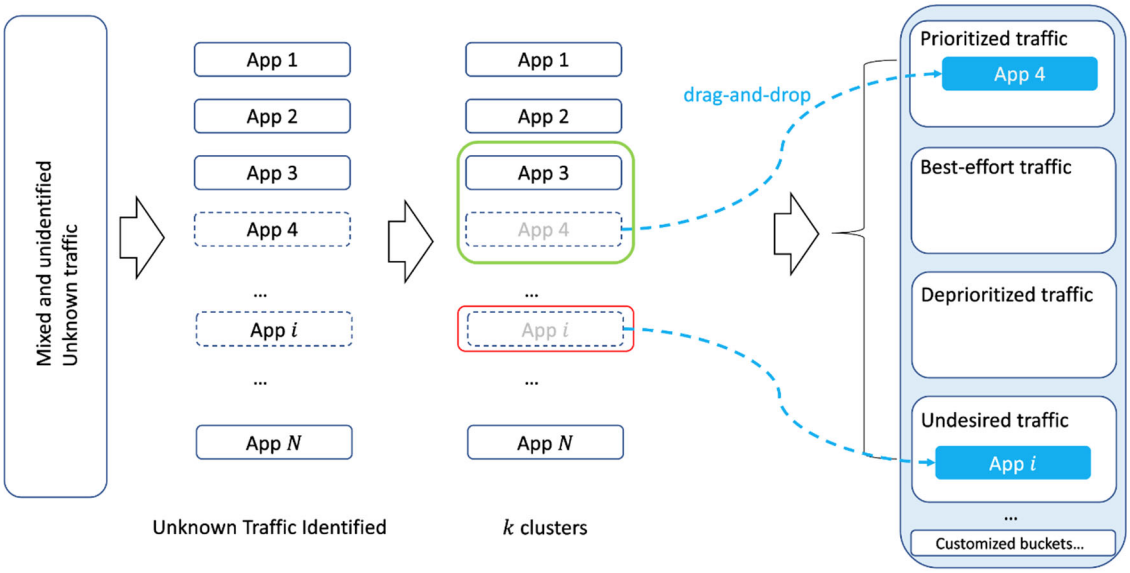

Figure 5 - Example drag-and-drop GUI Flow

In summary, the network management system proposed herein includes an Intent-Based Networking (IBN) Intent-recommender to classify unknown network traffic in a network environment using machine learning, including adjunct data. The network management system provides network administrators with full visibility of their network

so that they can properly define their intents for handling network traffic before using a typical IBN model. Based on the categorization of previously unknown network traffic, the IBN Intent-recommender provides suggestions for how the network administrators should define their intents. Network engineers will then choose whether to follow the suggestion to define their intent for a particular category of traffic flows. The recommendation system improves through a feedback loop that tracks whether the suggested intent for each unknown traffic flow cluster aligns with the specified intent of the network engineer. The feedback loop reinforces the decision of the network engineer in the machine learning model.

This network management system provides recommendations to network administrators on what intents to set, adding another intelligent layer to guide users before the translation step in traditional IBN. Providing useful, intelligent recommendations with maximum awareness and full visibility into network expands traditional IBN systems for network administrators. The network management system proposed herein provides an extra layer of security so that network administrators know exactly what kind of traffic is flowing through their network environment. Using this information, they can choose whether to follow the recommendations of the network management system to set their intents confidently. Thus, techniques presented herein can help to accelerate next-level IBN; expanding the system expands the current IBN by providing intelligent recommendations based on more accurately setting intents, thus providing maximum awareness/full visibility into a network.