Universidad del Istmo de Guatemala

Facultad de Ingeniería

Ingeniería en Sistemas y Ciencias de la Computación

Prácticas de Trabajo e Investigación 4

Dylan Gabriel Rodas Samayoa – rodas171315@unis.edu.gt

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**ACTIVIDAD LECTURA DE ARTÍCULOS**

**23 de Noviembre, 2018 – Preguntas Guía**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

ARTÍCULO I:

A Novel Approach for Network Attack Classification Based on Sequential Questions.

Preguntas guía:

¿Cuál es la hipótesis que se intenta comprobar con este estudio?

Las técnicas actuales de categorización de ataques protegen a un grupo específico de amenazas que ha desordenado toda la estructura de la taxonomía o es ambigua cuando los ataques de una red se combinan con otros ataques. Por lo tanto, surge la necesidad de crear un nuevo diseño de categorización viable para detectar ataques en la vida real.

¿Cuáles son las preguntas de investigación?

En el artículo, se propone un marco de detección de intrusiones y un esquema de agrupación de amenazas sobre la base de cuatro preguntas secuenciales ("Quién", "Dónde", "Cómo" y "Qué"). Dichas preguntas servirán para investigar y clasificar los ataques de red tradicionales para identificar el iniciador, la fuente, el estilo de ataque y la gravedad de un ataque.

¿Cuáles son los objetivos del artículo?

El desarrollo de una taxonomía de propósito general y común, proponiendo un modelo secuencial de categorización de preguntas y respuestas. Así como, proporcionar una lista preventiva de acciones para el administrador de la red, como una guía para reducir las consecuencias generales del ataque. Y, por último, recomendar una taxonomía diseñada para detectar ataques comunes en lugar de cualquier tipo particular de ataque que pueda tener un efecto práctico en la clasificación de ataques en la vida real.

¿Qué investigaciones se habían hecho antes sobre el tema?

Onik, M. M. H., Al-Zaben, N., Phan Hoo, H., & Kim, C. S. (2017). MUXER—A New Equipment for Energy Saving in Ethernet. Technologies, 5(4), 74.

Islam, M. M., Hassan, M. M., Alamri, A., & Huh, E. N. (2016). Data classification and scheduling for sensor virtualisation scheme in public healthcare system. International Journal of Sensor Networks, 22(4), 259-273.

¿Cómo contribuye este estudio a la disciplina?

El propósito de esta taxonomía mediante la nueva clasificación, es que puede ayudarnos a conocer más detalles sobre las características de ataque de la red, como los orígenes, los ámbitos, el iniciador y la gravedad de un ataque. También podemos planificar defensas efectivas y medidas preventivas, así como reducir las consecuencias de los ataques para las redes globales.

¿Cuáles son las fuentes de información utilizadas en este artículo?

Hay muchas investigaciones utilizadas como fuente de información sobre la base de clasificación de ataque de red empleadas en este artículo. Vulnerabilidades [1-2], listas de términos taxonomía [3], aplicación de taxonomía [4-7] y taxonomías multidimensionales [8-9], entre otras también importantes.

[1] Cohen, F. (1997). Information system attacks: A preliminary classification scheme. Computers & Security, 16(1), 29-46.

[2] Landwehr, C. E., Bull, A. R., McDermott, J. P., & Choi, W. S. (1993). A taxonomy of computer program security flaws, with examples (No. NRL/FR/5542--93-9591). NAVAL RESEARCH LAB WASHINGTON DC.

[3] Bishop, M. (1995). A taxonomy of unix system and network vulnerabilities. Technical Report CSE-95-10, Department of Computer Science, University of California at Davis.

[4] Rae, A., & Wildman, L. (2003). A taxonomy of attacks on secure devices. In Proceedings of the Australia Information Warfare and Security Conference 2003 (pp. 251-264). York.

[5] Álvarez, G., & Petrović, S. (2003). A new taxonomy of web attacks suitable for efficient encoding. Computers & Security, 22(5), 435-449.

[6] Wood, A. D., & Stankovic, J. A. (2004). A taxonomy for denial-of-service attacks in wireless sensor networks. Handbook of Sensor Networks: Compact Wireless and Wired Sensing Systems, 739-763.

[7] Mirkovic, J., & Reiher, P. (2004). A taxonomy of DDoS attack and DDoS defense mechanisms. ACM SIGCOMM Computer Communication Review, 34(2), 39-53.

[8] Lough, D. L. (2001). A taxonomy of computer attacks with applications to wireless networks (Doctoral dissertation, Virginia Tech).

[9] Howard, J. D., & Longstaff, T. A. (1998). A common language for computer security incidents (No. SAND98-8667). Sandia National Labs., Albuquerque, NM (US); Sandia National Labs., Livermore, CA (US).

¿Cuáles fueron los métodos utilizados en la investigación?

La clasificación se centra en cuatro procesos de ataque de red de preguntas secuenciales con: Quién, Dónde, Cómo y Qué. El enfoque se basa en la idea de que todos los ataques de red similares tienen una forma similar de atacar y la clasificación se construye con esas cuatro preguntas. Al seguir el proceso de ataque a la red desde el inicio hasta el final, este enfoque puede proporcionar un mejor enfoque que adapte todos los requisitos de una clasificación de ataque a la red, así como cubrir todos los ataques a la red actual de una manera sencilla que es muy útil para el futuro.

¿Cuáles son los datos presentados como evidencia en este artículo?

Se ha realizado una validación detallada del estudio y una comparación con otros trabajos para validación y justificación. El estudio ha identificado con éxito en detalle la clasificación de amenazas de riesgo como blaster, Melissa, Slammer, MS RPC Stack Overflow y Morris. La clasificación propuesta también satisfacía la mayoría de los requisitos necesarios para el desarrollo de una taxonomía de ataque.

¿Cuáles son las conclusiones principales del artículo?

La nueva metodología identificó las consultas comunes hacia una amenaza para detectar el comportamiento de los detalles y luego se clasifican en consecuencia. Con estas cuatro preguntas (Quién, dónde, cómo y qué), se puede reconocer claramente un tipo de ataque de red.

Se ha percibido que la fuente del ataque puede ser de solo o en grupo. De la misma manera, el método propuesto detectó que la amenaza puede propagarse desde múltiples fuentes, como una computadora, una unidad flash, un cable, WiFi, etc. Por último, la taxonomía propuesta detectada como consecuencia de un ataque puede ser una adquisición del control del sistema o simplemente afectar sin compartir con otros sistemas conectados.

La seguridad del sistema depende completamente de la detección de ataques y el mecanismo de seguridad posterior. Esto indica la necesidad de una taxonomía que proporciona información detallada sobre un ataque. Obviamente, la taxonomía de ataque centrada en preguntas progresivas propuestas puede exprimir ataques para extraer información detallada para ayudar a los administradores de sistemas.

ARTÍCULO II:

A SDN-based Flexible System for On-the-Fly Monitoring and Treatment of Security Events.

Preguntas guía:

¿Cuál es la hipótesis que se intenta comprobar con este estudio?

La ausencia de flexibilidad en el control del funcionamiento interno del equipo, así como el alto costo de la infraestructura existente, son barreras para la evolución de la arquitectura y la innovación necesaria en la provisión de nuevos servicios y aplicaciones de red. Una de las iniciativas en esta dirección es el paradigma de red definida por software (SDN) que en la mayoría de los casos se basa en el protocolo OpenFlow.

¿Cuáles son las preguntas de investigación?

Por lo general, SDN emplea un controlador para instalar, a pedido, reglas de reenvío de paquetes por flujo en los nodos de la red. A pesar de las ventajas aportadas por las redes SDN, algunas de las vulnerabilidades de las redes tradicionales persisten en las infraestructuras basadas en SDN, como la naturaleza típicamente centralizada del plano de control, que se suma al hecho de que muchas de las herramientas y técnicas utilizadas para la información de seguridad como el antivirus y el cortafuego no son suficientes para garantizar la seguridad. Las tecnologías de detección de intrusos, adecuadamente integradas con el entorno SDN, pueden proporcionar un elemento de seguridad adicional.

¿Cuáles son los objetivos del artículo?

El propósito del trabajo es, en primer lugar, extender los trabajos relacionados a través de la implementación de mecanismos flexibles adicionales para el monitoreo y tratamiento de los eventos de seguridad categorizados por tipo de ataque y asociados con los recursos de la lista blanca y la lista negra. En segundo lugar, la solución propuesta proporcionará mecanismos para realizar análisis de intrusión y ataques con validación mediante un testbed real de SDN-OpenFlow.

¿Qué investigaciones se habían hecho antes sobre el tema?

El uso de OpenFlow en el área de seguridad de la red considerando el análisis y la prevención de intrusiones ha sido discutido y ha presentado buenos resultados en investigaciones anteriores. Por ejemplo, Lopes et al. propone BroFlow, un IDPS (Sistema de Prevención de Detección de Intrusiones) elástico y distribuido para la defensa contra ataques DoS en SDN virtualizada, que se basa en la API de OpenFlow y el analizador de tráfico de red Bro. Jankowski et al. presentó una solución en la que el resultado se basaba en el supuesto de que es posible clasificar si los flujos de tráfico de la red representan una operación o ataque normal y la clasificación de los flujos se basa en las características obtenidas a través de la funcionalidad disponible en la tecnología SDN. Xing et al. presentó el SnortFlow, una propuesta de IPS en un entorno de nube, con XEN utilizando los interruptores OpenFlow para ayudar a capturar el tráfico. En este estudio, los autores desarrollaron un prototipo en el que se instaló el agente SnortFlow en las áreas Sun 0 y Dom U.

¿Cómo contribuye este estudio a la disciplina?

La propuesta del Sistema de Detección y Tratamiento de Intrusos (IDTS) con su enfoque de seguridad de redireccionamiento, mitigación y engaño del atacante innova y proporciona flexibilidad, particularmente en relación con la detección de intrusión actual utilizando un IDS en un estilo convencional. Esta técnica flexible, ahora asociada con un mecanismo de control de red (arquitectura SDN / OpenFlow), permite una forma innovadora, no solo para monitorear y detectar posibles ataques, sino también como una "reacción" a las amenazas de forma controlada y centralizada.

¿Cuáles son las fuentes de información utilizadas en este artículo?

[1] Anwer M. Bilal et al. Switchblade: A Platform for Rapid Deployment of Network Protocols on Programmable Hardware, ACM SIGCOMM Computer Communications Review, V. 40, No 4, pp 183-194, 2010.

[2] McKeown, N. et al. OpenFlow: Enabling Innovation in Campus Networks, SIGCOMM Computer Communications Review, V. 38, No 2, pp 69–74, 2008

[3] Kreutz, Diego; Rothenberg, Christian; Azodolmonlky, Siamak; Ramos, F. et al. Software-Defined Networking: A Comprehensive Survey, IEEE Proceedings, V. 103, No 1, pp. 14-76, 2015.

[4] Campos, Maxli; Martins, Joberto. A Security Architecture Proposal for Detection and Response to Threats in SDN Networks, IEEE Andean Council International Conference - ANDESCON, 2016.

[5] Bobba, Rakesh et al. Networking Software-Defined (SDN). Available in: <osetoreletrico.com.br/web/a-revista/edicoes/1786-redes-definidas-por-software-sdn.html>. October 2015.

[6] Lopes, Martin A et al. An Elastic Intrusion Detection System for Software Networks, Annals of Telecommunications, pp 1, 2016.

[7] Jankowksi, Damian; Amanowics, Marek. Intrusion Detection in Software Defined Networks with Self-Organized Maps Journal of Telecommunications and Information Technology, 2015.

[8] Xing, T. et al. Snort-Flow: A OpenFlow-based Intrusion Prevention System in Cloud Environment, Research and Educational Experiment Workshop - GREE, pp 89-92, 2013.

[9] Abelem, A.; Stanton, Michael; Machado, Iara; Martins, Joberto et al. FIT@BR - a Future Internet Testbed in Brazil. In: APAN (Asia Pacific Advanced Network) Network Research Workshop, V. 1, pp. 78-87, 2013.

¿Cuáles fueron los métodos utilizados en la investigación?

Se caracteriza como un estudio de caso aplicado que explora la capacidad de programación de los controladores SDN en un banco de pruebas real. El objetivo es validar la propuesta en sí misma y sus mecanismos implementados para la detección y reacción al uso futuro en la red FIBER de la Universidad de Salvador (UNIFACS).

¿Cuáles son los datos presentados como evidencia en este artículo?

Se presentó una breve descripción de las estrategias adoptadas e implementadas en el banco de pruebas real de la Red SDN y la validación de los mecanismos de protección. Los resultados obtenidos en las pruebas se presentaron como salidas de comando del controlador Ryu que se estaba ejecutando en modo detallado. La herramienta BASE se utiliza como herramienta de análisis para las alertas generadas por Snort y disponibles en el banco de pruebas de la red SDN real. Para toda la simulación de ataque detectada por Snort, se envía una alerta mediante el mensaje Packet\_event al controlador de red. El controlador a través de la aplicación mitigation.py extrae información de alerta buscando el flujo que coincide con la alerta que recibió la alerta.

¿Cuáles son las conclusiones principales del artículo?

En efecto, las pruebas de validación informadas ilustran solo algunos de los posibles enfoques de protección con la inclusión en la lista blanca y los enfoques de reacción con la inclusión en la lista negra y la señalización al administrador. Los trabajos futuros deben incluir el uso de otros IDS en una arquitectura con más de un conmutador OpenFlow para proporcionar equilibrio de carga entre otras alternativas potenciales. La flexibilidad del enfoque propuesto también refleja el hecho de que estamos proponiendo asegurar una red con una vista y un control lógicamente centralizados, aunque el controlador en sí mismo podría estar completamente distribuido y comúnmente adoptado en una red SDN / OpenFlow.

ARTÍCULO III:

Learning IoT in Edge: Deep Learning for the Internet of Things with Edge Computing.

Preguntas guía:

¿Cuál es la hipótesis que se intenta comprobar con este estudio?

El aprendizaje profundo es un enfoque prometedor para extraer información precisa de datos de sensores sin procesar de dispositivos IoT implementados en entornos complejos. Debido a su estructura multicapa, el aprendizaje profundo también es apropiado para el entorno informático de vanguardia.

¿Cuáles son las preguntas de investigación?

El aprendizaje profundo es una herramienta analítica sólida para grandes volúmenes de datos. En el Internet de las cosas (IoT), un problema abierto es cómo extraer de manera confiable los datos de IoT del mundo real de un entorno ruidoso y complejo que confunde las técnicas convencionales de aprendizaje automático. El aprendizaje profundo puede ser considerado como el enfoque más prometedor para resolver este problema.

¿Cuáles son los objetivos del artículo?

En este artículo, se busca introducir el aprendizaje profundo para IoT en el entorno informático de vanguardia. Dado que los nodos de borde existentes tienen una capacidad de procesamiento limitada, se propone el diseño de una nueva estrategia de descarga para optimizar el rendimiento de las aplicaciones de aprendizaje profundo de IoT con la computación de borde. En la evaluación de desempeño, se busca el desempeño de la ejecución de múltiples tareas de aprendizaje profundo en un entorno informático de vanguardia con la estrategia propuesta. Por último, que los resultados de la evaluación muestren que el método supera otras soluciones de optimización en el aprendizaje profundo para IoT.

¿Qué investigaciones se habían hecho antes sobre el tema?

L. Li, K. Ota, and M. Dong, “When Weather Matters: IoTBased Electrical Load Forecasting for Smart Grid,” IEEE Commun. Mag., vol. 55, no. 10, Oct. 2017, pp. 46–51.

L. Li et al., “Eyes in the Dark: Distributed Scene Understanding for Disaster Management,” IEEE Trans. Parallel Distrib. Systems, 2017. DOI: 10.1109/TPDS.2017.2740294.

¿Cómo contribuye este estudio a la disciplina?

Debido a su alta eficiencia en el estudio de datos complejos, el aprendizaje profundo jugará un papel muy importante en los futuros servicios de IoT. El modelo de aprendizaje profundo es muy apropiado para el entorno informático de borde, ya que es posible descargar partes de las capas de aprendizaje en el borde y luego transferir los datos intermedios reducidos al servidor de nube centralizado. Otra ventaja del aprendizaje profundo en computación perimetral es la preservación de la privacidad en la transferencia de datos intermedios.

¿Cuáles son las fuentes de información utilizadas en este artículo?

[1] Z. Fadlullah et al., “State-of-the-Art Deep Learning: Evolving Machine Intelligence Toward Tomorrow’s Intelligent Network Traffic Control Systems,” IEEE Commun. Surveys & Tutorials, DOI: 10.1109/COMST.2017.2707140.

[2] N. Kato et al., “The Deep Learning Vision for Heterogeneous Network Traffic Control: Proposal, Challenges, and Future Perspective,” IEEE Wireless Commun., vol. 24, no. 3, June 2017, pp. 146–53. DOI: 10.1109/ MWC.2016.1600317WC.

[10] N. D. Lane, P. Georgiev, and L. Qendro, “Deepear: Robust Smartphone Audio Sensing in Unconstrained Acoustic Environments Using Deep Learning,” Proc. 2015 ACM Int’l. Joint Conf. Pervasive and Ubiquitous Computing, 2015, pp. 283–94.

[12] S. Bhattacharya and N. D. Lane, “Sparsification and Separation of Deep Learning Layers for Constrained Resource Inference on Wearables,” Proc. 14th ACM Conf. Embedded Network Sensor Systems CD-ROM, ser. SenSys ‘16, 2016, pp. 176–89.

[13] M. A. Alsheikh et al., “Mobile Big Data Analytics Using Deep Learning and Apache Spark,” IEEE Network, vol. 30, no. 3, May/June 2016, pp. 22–29.

[15] C. Liu et al., “A New Deep Learning-Based Food Recognition System for Dietary Assessment on an Edge Computing Service Infrastructure,” IEEE Trans. Services Computing. DOI: 10.1109/TSC.2017.2662008.

¿Cuáles fueron los métodos utilizados en la investigación?

Primero se introdujo el aprendizaje profundo para IoT en el entorno informático de vanguardia. Este es un trabajo innovador que se enfoca en el aprendizaje profundo para IoT con computación avanzada. Formulando un modelo elástico para varios modelos de aprendizaje profundo para IoT en computación perimetral. Se diseñó un algoritmo en línea eficiente para optimizar la capacidad de servicio del modelo informático de vanguardia. Finalizando, con la prueba del modelo de aprendizaje profundo para IoT con experimentos extensos en un entorno informático de borde dado. Y comparando el método de computación de borde con soluciones tradicionales.

¿Cuáles son los datos presentados como evidencia en este artículo?

Los experimentos realizados, donde se eligieron 10 modelos CNN diferentes como redes de aprendizaje profundo y recopilación del tamaño de datos intermedio y la sobrecarga computacional de las aplicaciones prácticas de aprendizaje profundo. Los resultados de la evaluación de desempeño muestran que las soluciones pueden aumentar la cantidad de tareas implementadas en servidores perimetrales con requisitos de QoS garantizados.

¿Cuáles son las conclusiones principales del artículo?

Introducir el aprendizaje profundo de IoT en el entorno informático de vanguardia es la mejor opción para optimizar el rendimiento de la red y proteger la privacidad del usuario al cargar datos. La estructura de la computación perimetral reduce el tráfico de red de los dispositivos de IoT a los servidores en la nube, ya que los nodos perimetrales cargan datos intermedios reducidos en lugar de datos de entrada. Por último, se estableció la capacidad de servicio limitado de los nodos de borde y algoritmos para maximizar el número de tareas en el entorno de computación de borde.

ARTÍCULO IV:

Detecting Denial-of-Service Attacks from Social Media Text: Applying NLP to Computer Security.

Preguntas guía:

¿Cuál es la hipótesis que se intenta comprobar con este estudio?

El objetivo en el uso de las redes sociales está impulsado por la hipótesis de que, como un ataque de red, sus usuarios pasan por una serie de etapas de observación que pueden aprenderse y detectarse automáticamente.

¿Cuáles son las preguntas de investigación?

Este documento investiga una fuente para ataques múltiples con evidencia indirecta: texto de redes sociales. ¿Los usuarios de sistemas atacados publican en las redes sociales? ¿Qué se puede aprender de los comentarios? ¿Pueden los modelos de aprendizaje de PNL extraer suficiente información de las publicaciones de los usuarios para detectar ataques? El trabajo previo sobre detección de ataques con redes sociales es escaso y se enfoca en detectar palabras de tendencia. Este documento es el primero en aprender modelos de lenguaje sin diccionarios de "ataque" y palabras clave.

¿Cuáles son los objetivos del artículo?

El objetivo es la detección en tiempo real de ataques sin datos de red. El objetivo secundario es ilustrar las aplicaciones de PNL a temas de seguridad informática. La investigación sobre la extracción de información de las redes sociales ha demostrado que muchos tipos de eventos en el mundo pueden detectarse de manera confiable desde el idioma que los usuarios publican. Se han demostrado varios enfoques efectivos para identificar eventos como terremotos, conciertos y lanzamientos de productos y otros desastres naturales. Y detectar ataques DDoS no es muy diferente de estos objetivos, donde un ataque es un evento real en el mundo y toma por sorpresa a una comunidad. Este documento adopta así las ideas de la PNL, pero las aplica a la aplicación única de detección DDoS.

¿Qué investigaciones se habían hecho antes sobre el tema?

Hay muy poco trabajo previo en esta área, y lo que existe se enfoca completamente a las etapas posteriores, donde se convierten en comentarios directos a medida que la comunidad se une a la creencia de que un ataque es la causa. Ritter et al. (2015) propusieron modelos que incluyen palabras clave codificadas como "DDoS" y frases como "<entidad> está abajo". Su trabajo ayudó a identificar los ataques en las redes sociales, pero estas identificaciones tienden a ser después de que las noticias ya lo informaron. Los primeros síntomas que se discuten no usan palabras como "DDoS" porque aún no se ha llegado a la conclusión.

¿Cómo contribuye este estudio a la disciplina?

Se proponen los primeros modelos de aprendizaje que identifican las discusiones de ataques tempranos: el primero es una red neuronal y el segundo es un modelo temático más amplio que proporciona una mejor visión de la evolución de un ataque. Finalmente, se consigue modelar los temas y temas que los usuarios notan durante los ataques a la red.

¿Cuáles son las fuentes de información utilizadas en este artículo?

[1] Pramod Anantharam, Payam Barnaghi, Krishnaprasad Thirunarayan, and Amit Sheth. 2015. Extracting city traffic events from social streams. ACM Transactions on Intelligent Systems and Technology (TIST), 6(4):43.

[2] Edward Benson, Aria Haghighi, and Regina Barzilay. 2011. Event discovery in social media feeds. In Proceedings of the 49th Annual Meeting of the Association for Computational Linguistics: Human Language Technologies-Volume 1, pages 389–398. Association for Computational Linguistics.

[3] David A Broniatowski, Michael J Paul, and Mark Dredze. 2013. National and local influenza surveillance through twitter: an analysis of the 2012-2013 influenza epidemic. PloS one, 8(12):e83672.

[4] Weiwei Guo, Hao Li, Heng Ji, and Mona T Diab. 2013. Linking tweets to news: A framework to enrich short text data in social media. In ACL (1), pages 239– 249. Citeseer.

[5] Dennis Kergl. 2015. Enhancing network security by software vulnerability detection using social media analysis extended abstract. In Data Mining Workshop (ICDMW), 2015 IEEE International Conference on, pages 1532–1533. IEEE.

¿Cuáles fueron los métodos utilizados en la investigación?

Las contribuciones principales de este documento son las siguientes: (1) Una mejora del 25% sobre el trabajo anterior en la detección de ataques, (2) Presentación de los primeros resultados de la red neuronal en la detección de ataques de redes desde las redes sociales, (3) Presentación de una etiqueta parcialmente El modelo LDA para detectar ataques de red con resultados de vanguardia, (4) El PLDA permite el primer análisis de la evolución de un ataque visto a través de sus usuarios, y (5) Disposición la lista más grande de DDoS históricos Ataques hasta la fecha.

¿Cuáles son los datos presentados como evidencia en este artículo?

Este documento describe una aplicación novedosa de modelos de PNL para detectar ataques de denegación de servicio utilizando solo medios sociales como evidencia. Las redes individuales a menudo son lentas en los informes de ataques, por lo que un sistema de detección de datos públicos podría ayudar mejor a responder a un ataque amplio en múltiples servicios. Explorando métodos de PNL para usar los medios sociales como una medida indirecta del estado del servicio de red. Se describieron dos marcos de aprendizaje para esta tarea: una red neuronal de avance y un modelo LDA parcialmente etiquetado. Ambos modelos superan el trabajo anterior por márgenes significativos (20% de puntuación F1). Además, se mostró que el modelo basado en temas permite el primer análisis detallado de cómo reacciona el público ante los ataques de red en curso, descubriendo múltiples "etapas" de observación. Este es el primer modelo que detecta ataques a la red y proporciona un análisis de cuándo y cómo el público interpreta las interrupciones del servicio.

¿Cuáles son las conclusiones principales del artículo?

La conclusión central de los experimentos es que las redes sociales contienen señales para identificar ataques DDoS. La red neuronal propuesta superó el trabajo anterior (Motoyama et al., 2010) en un 20% de F1. Aunque los usuarios en línea son una fuente de evidencia indirecta, el 53% F1 de la red neuronal muestra que se puede extraer información útil del texto. Se puede mejorar aún más los resultados con el modelo de PLDAttack generativo basado en el modelado de temas, logrando un aumento menor del 4% en la red neuronal, pero del 25% en el enfoque de tendencias anteriores. Aunque las redes neuronales tienen ventajas significativas sobre los modelos basados ​​en LDA, PLDAttack ofrece ventajas al permitir un análisis más profundo de lo que dice la gente, los temas que se discuten y cómo las discusiones de ataque evolucionan con el tiempo en Twitter.