

**ĐẠI HỌC THÁI NGUYÊN**  
**TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG**

**ĐOÀN MINH CẢNH**

**NGHIÊN CỨU TỔNG QUAN NHỮNG VẤN ĐỀ AN NINH CHÍNH**  
**TRONG MẠNG INTERNET OF THINGS (IoT)**

**LUẬN VĂN THẠC SĨ KHOA HỌC MÁY TÍNH**

**Hướng dẫn khoa học: TS. Nguyễn Tuấn Minh**

**THÁI NGUYÊN, 2018**

## **LỜI CAM ĐOAN**

Tôi xin cam đoan đây là công trình nghiên cứu khoa học độc lập của riêng tôi. Các số liệu sử dụng phân tích trong luận án có nguồn gốc rõ ràng, đã công bố theo đúng quy định. Các kết quả nghiên cứu trong luận án do tôi tự tìm hiểu, phân tích một cách trung thực, khách quan và phù hợp với thực tiễn của Việt Nam. Các kết quả này chưa từng được công bố trong bất kỳ nghiên cứu nào khác.

**Học viên thực hiện**

**Đoàn Minh Cảnh**

## LỜI CẢM ƠN

Em xin được cảm ơn sâu sắc đến Thầy giáo TS. Nguyễn Tuấn Minh đã tận tình hướng dẫn khoa học cho em trong suốt thời gian vừa qua. Thầy luôn động viên giúp đỡ em hoàn thành luận văn một cách nhanh nhất, đúng tiến độ. Một lần nữa xin được cảm ơn đến thầy, chúc thầy luôn mạnh khỏe và công tác tốt trong sự nghiệp trồng người. Em cũng xin cảm ơn các Thầy, Cô đã tham gia giảng dạy em tại Nhà trường, giúp em có được lượng kiến thức, phương pháp học tập và nghiên cứu phù hợp cho chuyên ngành của mình.

Em cũng xin gửi lời cảm ơn đến Gia đình, bạn bè và tất cả những người thân của em đã động viên giúp đỡ em để em hoàn thành được luận văn này.

**Học viên thực hiện**

**Đoàn Minh Cảnh**

## MỤC LỤC

LỜI CAM ĐOAN .....	i
LỜI CẢM ƠN .....	iii
MỤC LỤC.....	iv
DANH MỤC CHỮ VIẾT TẮT .....	vi
DANH MỤC HÌNH ẢNH .....	x
MỞ ĐẦU.....	1
CHƯƠNG 1: TỔNG QUAN VÀ AN TOÀN BẢO MẬT TRONG IOTS.....	5
1.1. Khái niệm công nghệ IoTs.....	5
1.2 Một số ứng dụng trong công nghệ IoTs.....	9
1.2.1. Trong giao thông:.....	9
1.2.2 Thành phố thông minh:.....	10
1.2.3. Trong chăm sóc sức khỏe: .....	10
1.2.4. Nhà thông minh: .....	11
1.2.5. Trong phạm trù cá nhân và xã hội: .....	12
1.2.6. Môi trường thông minh:.....	13
1.2.7. Điều khiển trong công nghiệp: .....	13
1.2.8. Nông nghiệp thông minh: .....	14
1.3. Tầm quan trọng của bảo mật IoTs. ....	14
1.4. Nguy cơ hệ thống và các hình thức tấn công.....	15
1.4.1. Nguy cơ hệ thống.....	15
1.4.2. Các hình thức tấn công mạng. ....	16
1.5. Kết chương 1 .....	21
CHƯƠNG 2: KIẾN TRÚC CƠ SỞ HẠ TẦNG VÀ CÁC KỸ THUẬT AN NINH CHỦ YẾU TRONG IOTS .....	22
2.1. Kiến trúc an ninh trong IoTs.....	22
2.1.1. Đặc điểm an ninh .....	23
2.1.2. Yêu cầu an ninh .....	23

2.2. Các kỹ thuật an ninh chủ yếu.....	25
2.2.1. Kỹ thuật mã hóa.....	26
2.3. Kỹ thuật bảo mật dữ liệu cảm biến không dây .....	32
2.3.1. Hệ thống an ninh RFID.....	32
2.3.2. Bảo mật mạng an ninh cảm biến.....	34
2.4. Kỹ thuật bảo mật thông tin liên lạc.....	35
2.4.1. Bảo mật thu thập Thông tin .....	35
2.4.2. Bảo mật xử lý thông tin .....	36
2.4.3. Bảo mật truyền thông tin .....	36
2.4.4. Bảo mật ứng dụng thông tin .....	37
2.5. Kết chương 2.....	42
<b>CHƯƠNG 3: MỘT SỐ THÁCH THỨC CÙNG HƯỚNG PHÁT TRIỂN TRONG TƯƠNG LAI VÀ ỨNG DỤNG BẢO MẬT IOTS DỰA TRÊN CÔNG NGHỆ LẤY MẪU NÉN .....</b>	<b>42</b>
3.1. Thách thức và hướng phát triển .....	42
3.1.1. Thách thức .....	42
3.2.2. Hướng phát triển tương lai.....	48
3.2. Tăng cường bảo mật trong hệ thống iots dựa trên công nghệ lấy mẫu nén.....	51
3.2.1. Công nghệ lấy mẫu nén .....	52
3.2.2. Thuật toán xử lý dữ liệu dựa trên biến đổi wavelet.....	53
3.2.3. Thuật toán xử lý dữ liệu dựa trên công nghệ lấy mẫu nén (cs) .....	55
3.3. Kết chương 3.....	58
<b>KẾT LUẬN .....</b>	<b>58</b>
<b>TÀI LIỆU THAM KHẢO.....</b>	<b>59</b>

## DANH MỤC CHỮ VIẾT TẮT

IoTs	Internet of Things	Mạng lưới vạn vật kết nối Internet
RFID	Radio Frequency Identification	Nhận dạng tần số vô tuyến
IIoTs	Industrial Internet of Things	Cấu trúc Internet of Things
IP	Internet Protocol	Giao thức mạng
IoM	Internet of Media	Mạng đa phương tiện
IoS	Internet of Services	Dịch vụ mạng
MEMS	Microelectromechanical system	Hệ vi điện cơ
RF	Radio Frequency	Tần số vô tuyến
LF	Low frequency	Dải tần số thấp
WSNs	Wireless sensor network	Mạng cảm biến không dây
MAC	Medium Access Control	Điều khiển truy nhập truyền thông
WPAN	Wireless Personal Area Networks	Mạng cá nhân không dây
RSN	Network sensor RFID	Mạng cảm biến nhận dạng tần số vô tuyến điện
NFC	Near Field Communication	Giao thức giao tiếp trường gần
BLE	Bluetooth Low Energy	Bluetooth năng lượng thấp
PHY	Physical layer	Lớp vật lý
GATT	Generic Access Profile	Cấu hình truy cập chung
Wifi	Wireless Fidelity	Wifi
LAN	Local Area Network	Mạng cục bộ
LR-WPAN	Low rate- wireless private area networks	Mạng tư nhân không dây tốc độ thấp
QoS	Quality of Service	Chất lượng dịch vụ
DSSS	Direct sequence spread	Phương pháp trực tiếp phổ chuỗi lây

	spectrum	lan
PAN	Personal Area Networks	Mạng cá nhân
LTE	Long-Term Evolution	Phát triển dài hạn
LTE-A	Long Term Evolution Advanced	Phát triển tiên hóa dài hạn
MTC	Machine Type Communication	Loại máy truyền thông
OFDM A	Orthogonal Frequency Division Multiple Access	Phân chia đa truy nhập tần số trực giao
PRB	Physical resource blocks	Khối tài nguyên vật lý
RAN	Radio Access Network	Mạng truy nhập vô tuyến
CN	Core Network	Mạng lõi
MTCG	MTC gate	Cổng MTC
RTOS	Real Time Operating System	Hệ thống điều hành thời gian thực
BAS	Building Automation Systems	Hệ thống tự động hóa
ITS	Intelligent Transport System	Hệ thống giao thông thông minh
T-CPS	Transportation Cyber Physical Systems	Hệ thống vật lý máy ảnh trong giao thông vận tải
RDF	Resource Description Framework	Khung mô tả nguồn
EXI	Efficient XML Interchange	Sự trao đổi XML hiệu quả
XML	Extensible Markup Language	Mở rộng ngôn ngữ đánh dấu
CoAP	Constrained Application Protocol	Giao thức ứng dụng ép buộc
REST	Representational State Transfer	Chuyển đổi trạng thái biểu diễn
HTTP	Hypertext Transfer Protocol	Giao thức siêu chuyển đổi

UDP	User Datagram Protocol	Giao thức dữ liệu người dùng
DTLS	Datagram TLS	Bảo mật lớp vận chuyển dữ liệu
MQTT	Message Queue Telemetry Transport	Chuyển giao từ xa dòng bản tin
TCP	Transmission Control Protocol	Giao thức điều khiển truyền vận
XMPP	Extensible Messaging and Presence Protocol	Bản tin mở rộng và giao thức hiện tại
IM	instant messaging	Tin nhắn nhanh
AMQP	Advanced Message Queuing Protocol	Giao thức hàng đợi bản tin cấp cao
DDS	Data Distribution Service	Dịch vụ phân phối dữ liệu
OMG	Object Management Group	Nhóm Quản lý đối tượng
DCPS	Data-Centric PublishSubscribe	Trung tâm dữ liệu theo dõi công khai
DLRL	Data-Local Reconstruction Layer	Lớp tái tạo dữ liệu cục bộ
RPL	Routing Protocol for Low Power and Lossy Networks	Giao thức định tuyến cho mạng suy hao và mạng công suất thấp
DAO	Destination Advertisement Object	Đối tượng đến đích
6LowPAN	Low power Wireless Personal Area Networks	Mạng cá nhân không dây công suất thấp
HAN	Home Automation Networks	Mạng tự động trong nhà
TLS	Transport Layer Security	Bảo mật lớp vận chuyển
API	Application Programming Interfaces	Giao thức lập trình ứng dụng
OEM	Original Equipment	Sản xuất thiết bị nguồn



	Manufacturers	
ISP	Internet service provider	Nhà cung cấp dịch vụ Internet
ETSI	European Telecommunications Standards Institute	Viện Tiêu chuẩn Viễn thông châu Âu
PMI	Physical Mobile Interaction	Giao diện di động lớp vật lý
ERP	Enterprise Resource Planning	Hoạch định nguồn lực doanh nghiệp
CIM	City Information Model	Mô hình thông tin thành phố
W3C	World Wide Web Consortium	Nhiệm vụ hướng dẫn World Wide Web
IETF	Internet Engineering Task Force	Lực lượng đặc nhiệm kỹ thuật Internet
IEEE	EPCglobal IEEE	Viện kỹ nghệ Điện và Điện Tử EPCglobal
ETSI	European Telecommunications Standards Institute	Viện Tiêu chuẩn Viễn thông châu Âu
ICT	Information and Communications Technology.	Công nghệ thông tin và truyền thông
TTDL	Data Center Downtime	Trung tâm dữ liệu

## DANH MỤC HÌNH ẢNH

Hình 1: Tổng quan Internet of things (IoTs).....	12
Hình 1.1: Mọi vật đều có thể được kết nối.....	15
Hình 1.2: Tương tác của mạng lưới thiết bị kết nối Internet.,.....	17
Hình 1.3: Mô hình thu thập mật độ và cảnh báo tắc nghẽn giao thông.....	19
Hình 1.4: Mô hình chăm sóc sức khỏe.....	20
Hình 1.5: Mô hình hệ thống nhà thông minh.....	21
Hình 1.6: Cá nhân và xã hội.....	22
Hình 1.7: kỹ thuật đánh lừa.....	27
Hình 1.8: Tấn công DdoS.....	29
Hình 1.9: Tấn công chuyển tiếp lựa chọn.....	29
Hình 1.10: Tấn công Wormhole.....	30
Hình 2.1: Xây dựng kiến trúc an ninh trong IoTs.....	31
Hình .2.2: Mã hóa đối xứng.....	36
Hình 2.3: Mã hóa bất đối xứng.....	38
Hình 2.4: Giao thức Secure Socket Layer (SSL).....	48
Hình 2.5: Giao thức Secure Socket Layer (SSL).....	49
Hình 3.1: Dữ liệu cảm biến nhiệt độ thu từ 2000 bộ cảm biến trong hệ thống IoTs.....	62
Hình 3.2: Dữ liệu cảm biến sau biến đổi Wavelet sẽ trở thành các hệ số lớn và còn lại là các hệ số bé có thể coi bằng không ('0').....	62
Hình 3.3: Hệ số lớn tăng và chất lượng khôi phục dữ liệu trong các môi trường có nhiều và không có nhiễu.....	63
Hình 3.4: Sử dụng hai cơ sở là Wavelet và DCT để làm rộng dữ liệu trong quá trình khôi phục dữ liệu với công nghệ nén cảm biến.....	64
Hình 3.5: Hình ảnh được chọn để thực hiện mô phỏng nén và khôi phục dữ liệu sử dụng công nghệ lấy mẫu nén.....	65